



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**AN INVESTIGATION OF NETWORK ENTERPRISE RISK
MANAGEMENT TECHNIQUES TO SUPPORT MILITARY
NET-CENTRIC OPERATIONS**

by

John F. Teply

September 2009

Thesis Advisor:
Second Reader:

Edouard Kujawski
Jean Johnson

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE An Investigation of Network Enterprise Risk Management Techniques to Support Military Net-Centric Operations			5. FUNDING NUMBERS	
6. AUTHOR(S) John F. Teply				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) None			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) System security and information assurance requirements and specifications incorporated into the architectural design of a network enterprise must be driven by an adaptable and evolving network enterprise risk management plan. Network Risk Management must start at concept design and relate to the network's Concept of Operations. The purpose of this thesis is to examine some of the essential elements necessary in a network enterprise risk management plan for a complex global networked system similar to the Global Information Grid (GIG). It compares the current Department of Defense (DoD) framework for risk management with other popular network risk management process models. An important but difficult part of the risk management process is determining the value of network assets. Another important, but overlooked element of risk management processes, is evaluating the network for resiliency; the ability to return to normal in time to prevent the compromise of a mission. The contention is that risk management planning must include planning for network survivability and resiliency. Selected elementary network architectures are analyzed for attributes of the architectures that promote information assurance qualities of confidentiality, integrity, and availability. Finally, recommendations are made on applying important elements of network risk management into the conceptual architecture of a global network.				
14. SUBJECT TERMS Network Enterprise Risk Management, Network Survivability and Resiliency, Vulnerability, Threat, Impact, Global Information Grid			15. NUMBER OF PAGES 187	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**AN INVESTIGATION OF NETWORK ENTERPRISE RISK MANAGEMENT
TECHNIQUES TO SUPPORT MILITARY NET-CENTRIC OPERATIONS**

John F. Teply
Contractor, Cubic Applications, Inc., San Diego, CA
B.S., United States Naval Academy, 1972
M.S., Naval Postgraduate School, 1980

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2009**

Author: John F. Teply

Approved by: Edouard Kujawski, PhD
Thesis Advisor

Jean Johnson, MSSE
Second Reader

David Olwell, PhD
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

System security and information assurance requirements and specifications incorporated into the architectural design of a network enterprise must be driven by an adaptable and evolving network enterprise risk management plan. Network Risk Management must start at concept design and relate to the network's Concept of Operations. The purpose of this thesis is to examine some of the essential elements necessary in a network enterprise risk management plan for a complex global networked system similar to the Global Information Grid (GIG). It compares the current Department of Defense (DoD) framework for risk management with other popular network risk management process models. An important but difficult part of the risk management process is determining the value of network assets. Another important, but overlooked, element of risk management processes, is evaluating the network for resiliency; the ability to return to normal in time to prevent the compromise of a mission. The contention is that risk management planning must include planning for network survivability and resiliency. Selected elementary network architectures are analyzed for attributes of the architectures that promote information assurance qualities of confidentiality, integrity, and availability. Finally, recommendations are made on applying important elements of network risk management into the conceptual architecture of a global network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
	1. Information Technology Evolution	1
	2. Information Technology Today	2
	3. Future Vision of Information Technology	2
	4. Architectural Vision for Networked Information Systems.....	3
	5. Challenges.....	5
	a. <i>Architecture</i>	5
	b. <i>GAO Concerns</i>	6
	c. <i>Space and Naval Warfare Command Concerns</i>	8
	6. Service Networks Integration into the GIG.....	9
B.	PURPOSE.....	11
	1. After the Fact Risk Management Diminishes Network Capability.....	11
	2. Summary of Purpose	13
C.	RESEARCH QUESTIONS.....	13
D.	BENEFITS OF THIS STUDY	14
E.	SCOPE AND METHODOLOGY	14
II.	APPLICATION OF SYSTEMS ENGINEERING PRINCIPLES TO NETWORK ENTERPRISE ARCHITECTING.....	17
A.	INTRODUCTION.....	17
B.	NETWORK CHARACTERISTICS	20
	1. Attributes of a Network.....	20
	2. Network Quality of Service Attributes	23
C.	NETWORK HARDWARE ARCHITECTING	24
	1. Bus Topology	25
	2. Ring Topology	26
	3. Star Topology	26
	4. Tree Topology.....	27
	5. Mesh Topology	27
D.	NETWORK SOFTWARE ARCHITECTING	28
	1. Open Architecture	29
	a. <i>Open Architecture Computing Environment (OACE)</i>	29
	b. <i>Vulnerability of Open Architecture</i>	32
	2. Overlay Networks	32
	3. Service Oriented Architecture	33
	a. <i>Service Oriented Architecture Direction for the Military</i>	33
	b. <i>Service Oriented Architecture Definitions</i>	34
	c. <i>Distributing Services under Service Oriented Architecture</i> ..	35
	d. <i>Advantages of SOA</i>	37
	e. <i>Challenges of Service Oriented Architecture</i>	38

E.	NETWORK ARCHITECTURAL VULNERABILITIES WITHIN NETWORK LAYERS	39
1.	ISO Model.....	39
2.	Vulnerabilities and Mitigating Strategies within the ISO Layers.....	40
F.	SUMMARY: NETWORK ARCHITECTURAL CONSIDERATIONS IN MANAGING NETWORK RISK.....	42
III.	RISK MANAGEMENT OVERVIEW	45
A.	INTRODUCTION.....	45
B.	RISK CATEGORIES AND DEFINITIONS	45
1.	Risk.....	45
a.	<i>Safety Risk</i>	46
b.	<i>Financial and Program Risk</i>	46
c.	<i>Operational Risk</i>	47
d.	<i>Enterprise Risk</i>	48
2.	Risk Analysis	49
a.	<i>Risk Identification</i>	49
b.	<i>Risk Assessment</i>	49
3.	Risk Management	50
a.	<i>Risk Mitigation Planning</i>	50
b.	<i>Risk Mitigation Implementation and Plan of Action</i>	51
c.	<i>Risk Management Plan Tracking</i>	51
C.	DECISION-MAKING PROCESS.....	51
1.	Risk Factors/Influence.....	51
a.	<i>Influence</i>	51
b.	<i>Uncertainty</i>	55
D.	THE DOD RISK MANAGEMENT PROCESS.....	56
1.	DoD Risk Identification.....	57
2.	DoD Qualitative Risk Analysis	58
3.	DoD Risk Mitigation Planning.....	59
4.	DoD Risk Mitigation Plan Implementation.....	59
5.	Risk Tracking.....	60
E.	SUMMARY	60
1.	Benefits of the Risk Management Process.....	60
2.	Relating the Process to the Network Enterprise	61
3.	Relating Benefits to Costs.....	61
IV.	ENTERPRISE NETWORK RISK MANAGEMENT.....	63
A.	INTRODUCTION.....	63
B.	RISKS IN THE NETWORK ENVIRONMENT	64
1.	Safety Risk	65
2.	Operational Risk	65
3.	Enterprise Risk.....	66
C.	RISK CONTROL IN A NETWORK.....	67
1.	Balancing Security with Functionality is a Team Effort.....	67

	2.	Controlling Risk is an Evolutionary Process Requiring Several Iterations.....	67
D.		RISK MANAGEMENT OF A GLOBAL NETWORK ENTERPRISE ...	68
	1.	Complexity of Network Risk Management for an Enterprise System	68
	2.	Beginning the Process Early in a Network System's Lifecycle.....	69
E.		PROPOSED NETWORK ENTERPRISE RISK MANAGEMENT PROCESS (NERMP).....	70
	1.	Review of Available Software Risk Management Processes.....	70
	2.	NERMP Details	71
F.		IDENTIFYING, EVALUATING AND MEASURING THE ELEMENTS OF RISK ANALYSIS AND ASSESSMENT.....	74
	1.	Asset Valuation.....	74
	2.	Vulnerability Determinations	76
	3.	Threat Assessment	79
	4.	System Recovery	82
G.		ATTACK TREES: A USEFUL TOOL IN RISK IDENTIFICATION AND ASSESSMENT	83
	1.	Identifying and Correcting Vulnerabilities	84
	2.	Minimal Cut Sets.....	86
	3.	Identifying and Analyzing Threat Motivations and Constraints ..	86
H.		SUMMARY	88
V.		NETWORK SURVIVABILITY AND RESILIENCY	89
A.		INTRODUCTION.....	89
B.		DEFINING SURVIVABILITY AND RESILIENCE	90
	1.	Network Survivability Characteristics	90
	a.	<i>Susceptibility</i>	90
	b.	<i>Vulnerability</i>	91
	c.	<i>Recoverability</i>	91
	2.	Designing a Network for Survivability	92
	a.	<i>Designing Survivable Networks at the System Boundaries...</i>	92
	b.	<i>Designing Survivable Systems with COTS Software</i>	93
	c.	<i>An Example of Survivability and Resiliency Scenario-Driven Requirements</i>	94
	d.	<i>Challenges in Quantifying Survivable Network and Software Attributes</i>	96
C.		ARCHITECTING SURVIVABLE NETWORKS	97
	1.	Network Attribute Considerations.....	97
	a.	<i>Consequences</i>	98
	b.	<i>Connectivity</i>	98
	c.	<i>Control</i>	99
	d.	<i>Governance</i>	99
	e.	<i>Communication</i>	100
	2.	Elements in the Architecture of a Survivable Network.....	101
	a.	<i>Usage Models</i>	101

b.	<i>Fault Tolerance</i>	102
D.	SURVIVABILITY MODELING	106
1.	Reactive Risk Analysis.....	106
2.	Modeling the Recovery Phase of a Survivable Network	107
3.	Characteristics of Dynamic Mobile Networks	109
E.	SUMMARY	109
VI.	CONCLUSIONS	113
A.	SUMMARY	113
1.	Network Architecture	114
2.	Network Risk Management	115
3.	Network Survivability and Resilience	115
4.	Network Enterprise Risk Management	116
B.	RECOMMENDATIONS OF AREAS FOR FURTHER RESEARCH ..	117
APPENDIX A.	VULNERABILITY AND MITIGATION STRATEGIES BY NETWORK LAYER	119
A.	INTRODUCTION	119
B.	NETWORK ISO LAYERS AND THE RISKS TO NETWORK QOS ATTRIBUTES	120
1.	Physical Layer	120
2.	Data Link Layer	122
3.	Network Layer	123
4.	Transport Layer.....	124
5.	Session Layer	125
6.	Presentation Layer.....	127
7.	Applications Layer.....	128
C.	SUMMARY	129
APPENDIX B.	OVERVIEW OF SOME CURRENT RISK MANAGEMENT PROCESS MODELS AND THEIR APPLICABILITY TO NETWORKS	131
A.	INTRODUCTION	131
B.	DESCRIPTIONS OF CURRENT MODELS AND THEIR APPLICABILITY	132
1.	Information Assurance Risk Management (IARM) (Safety Risk)	132
2.	Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)	133
3.	Fundamental Information Risk Management (FIRM)	134
4.	Simple to Apply Risk Analysis (SARA) and Simplified Process for Risk Identification (SPRINT)	134
5.	Cobra.....	135
6.	The CORAS Method.....	135
7.	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	136
8.	Architecture Refinement Process	138
9.	Mission Assurance Analysis Protocol (MAAP).....	139

10.	Network Risk Analysis Method (NetRAM).....	140
11.	Mission Oriented Risk and Design Analysis (MORDA)	143
C.	SUMMARY	146
APPENDIX C. FORMULATION OF THE COST/BENEFIT MODEL FOR		
	REACTIVE RISK ANALYSIS	147
A.	MODEL DERIVATION	147
B.	MODEL FORMULATION.....	149
LIST OF REFERENCES		151
INITIAL DISTRIBUTION LIST		157

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	GIG Federated Architecture (From: DoD CIO, 2007).....	4
Figure 2.	GIG core Services and Underlying SOA Infrastructure (From: DoD CIO, 2007)	6
Figure 3.	Communications Infrastructure of the GIG (From: DoD CIO, 2007)	10
Figure 4.	Relationship between Diameter and Aggregation in a Network	22
Figure 5.	OA Layered Approach (From: Naval Surface Warfare Center, 2004).....	30
Figure 6.	Example of Network Overlay (From: Google Network Pictures, 2009)	33
Figure 7.	Service Oriented Architecture Arrangement (From: Geholt, 2009)	35
Figure 8.	A Conception of SOA in Defense Applications (From: Gehlot, 2009).....	36
Figure 9.	Graphical Interpretation of Network Layer Abstractions	40
Figure 10.	Basic Influence Diagram on Risk to a Network	52
Figure 11.	Multiple Objective Influence Diagram on Risk to a Network	54
Figure 12.	DoD Risk Management Process (From: DoD RMG, 2006)	57
Figure 13.	DoD Risk Reporting Matrix (From: DoD RMG, 2006)	58
Figure 14.	Network Enterprise Risk Management Process (NERMP)	71
Figure 15.	Sample Attack Tree Analysis of a Threat	85
Figure 16.	The Attack Tree from the Attacker's Perspective.....	87
Figure 17.	ISO Network Layers Mapped to FORCENet Network Model (From: Stewart, 2006).....	120
Figure 18.	An Example of Tunneling at the Data Link Layer with Ethernet (From: May, 2004).....	123
Figure 19.	The OCTAVE Risk Management Cycle (From: Caralli & Young, 2008)	137
Figure 20.	The 10 Modules of the NetRAM Framework (From: Hamdi & Bordiga, 2005)	142

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Network Vulnerability and Mitigating Strategies within Network Layers.....	41
Table 2.	Effects on Network Security due to Evolutionary Change (From: Mulokey, 2009).....	68

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

ANSI	American National Standards Institute
C4I	Command, Control, Communications, Computers & Intelligence
CCTA	Central Computer and Telecommunications Agency
CERT	Computer Emergency Response Team
CMMI	Capability Maturity Model Integration
CNCI	Comprehensive National Cyber-security Initiative
CORBA	Common Object request Broker Architecture
COTS	Commercial Off the Shelf
CRAMM	CCTA Risk Analysis and Management Method
DDoS	Distributed Denial of Service
DDS	Data Distribution Service
DISA	Defense Information Systems Agency
DNS	Domain Name Server
DoD	Department of Defense
EBAO	Effects-Based Approach to Operations
FDDI	Fiber Distributed Data Interface
FIRM	Fundamental Information Risk Management
FMECA	Failure Mode, Effects and Criticality Analysis
GAO	U.S. Government Accountability Office
GCCS	Global Command and Control System
GIG	Global Information System
HTTP	Hyper-text Transmission Protocol
IA	Information Assurance
IARM	Information Assurance Risk Management
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Standardization Organization
LAN	Local Area Network

MAAP	Mission Assurance Analysis Protocol
MAN	Metropolitan Area Network
MORDA	Mission Oriented Risk and Design Analysis
NAT	Network Address Translator
NCO	Net-centric Operations
NCW	Net-centric Warfare
NERMP	Network Enterprise Risk Management Process
NetRAM	Network Risk Analysis Method
NSA	National Security Agency
OACE	Open Architecture Computing Environment
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OMG	Object Management Group
QoS	Quality of Service
SARA	Simple to Apply Risk Analysis
SEI/CMU	Software Engineering Institute of Carnegie-Mellon University
SOA	Service Oriented Architecture
SOCRATES	Security Optimization Countermeasure Risk and Threat Evaluation System
SONET	Synchronous Optical Network
SoS	System of Systems
SPRINT	Simplified Process for Risk Identification
TCP	Transmission Control Protocol
UDDI	Universal Description, Discovery & Integration
UDP	Universal Datagram Protocol
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

EXECUTIVE SUMMARY

The Department of Defense and the military services have clearly articulated their vision of information operations and the use of networking as the future strategy for military operations based on knowledge superiority. Computers and the automated processing capability inherent in them used to be seen as one of the technology tools in a tool set to increase the effectiveness of major weapons platforms and maneuver warfare, including increasing capability in operations, training, logistics, and communications within the different warfare areas. Today, that vision has expanded to raise the precedence of information technology and networking power and put it in a warfare area of its own. Information and its collection, manipulation, distribution, use, and protection are considered vital to the future of warfare and are central to the defense strategy of the nation. Concomitant with the increase of importance of information superiority, and Net-centric Operations, the reality is that the systems that make this vision a reality are continuously threatened by malicious entities that use viably ingenious ways to gain access to those information systems; disrupt and deny valid users access; and steal, fabricate or distort the programs and data resident in these systems. To make the Global Information Grid (GIG) a reality, DoD must follow rigorous discipline in systems engineering principles and a robust risk management process, translating desired capabilities into detailed requirements and specifications that drives the architecture of the global network. This is no small task. The complexity and expense of tying together legacy and developing systems into a global network that connect with diverse state-of-the-art communications links is a huge endeavor. The network is populated by tremendous amounts of data, which interface and interoperate with many systems of varying functionality. The network is intended to provide the right information at all levels of command. Security requirements drive the architecture of the GIG network as well.

This thesis investigates possible solutions to concerns of the U.S. Navy leadership with regard to network enterprise operations and security protection procedures, focusing on the following network enterprise risk management issues.

- The considerations in developing and improving network enterprise risk management planning implementation of the processes presently used by DoD and the military services for their information systems and networks on the global domain as Net-Centric Operations, Net-Centric Warfare, and Information Dominance.
- The attributes of a robust network enterprise risk management program and how it should be implemented so that it supports the confidentiality, availability, integrity, reliability, and trustworthiness of the military's critical information resources so they act as an enabler to mission success.
- Some of the architectural implications in the design of hardware (topology) and software (network management and control) and the process imperatives in the operation of networked information systems that make a global network system survivable and resilient to attack from hostile forces.
- Some of the popular risk management processes in the public domain and how their methodology might enhance DoD's network enterprise risk management process to achieve a survivable and resilient enterprise network and make decisions on the cost/benefit or value of the choices in implementing network security measures, ensuring quality of service and information assurance.

NETWORK ARCHITECTURE

Networks are architected in different arrangements to provide different capabilities while efficiently using available resources. The way a network is architected can introduce vulnerabilities through the make-up of the network components, by the way the components are connected, and by the methods employed and the layer of the network where they are employed to provide protection for network and information assets. No matter how elegant the architecture of a network, designed to provide a set of services, a network compromised by the enemy could affect operations from mission degradation to mission failure; from the top level of the chain of command to the tactical units in the field. As network vulnerabilities are discovered and an assessment of the risks associated with those vulnerabilities is conducted, it is important to determine what network quality of service attributes that U.S. protection services and countermeasures (technological, procedural, or managerial) seek to secure or enhance through the protection of data and program resources, and how these attributes can be secured through innovative system design and network architecting. It is important in the

development and operation of a network (as well as any system) to learn how vulnerabilities are created and how they are discovered. This information provides system developers with valuable experience to draw upon when developing follow-on systems

The topological arrangement of a network is the hardware architecture, and different topologies introduce different vulnerabilities. Mesh network architecture offers the network superior resilience from attack, but these systems are costly and complex to set up. The software network management of a mesh network can be quite convoluted and it is hard to monitor the effectiveness of the management and security of the network. However, if the threat of attack against the value of the assets in this type of network is high, the cost and the complexity of design and installation may be worth it. The GIG is a combination of many architectural topology arrangements, riding on the backbone of the Defense Information Systems Agency (DISA) intranet bus. For this reason, a comprehensive enterprise risk management program has to consider the GIG architecture from the top down in aggregation and from the bottom up as each type of topology used in interconnecting networks affects the enterprise vulnerability picture. The architectural framework of the GIG and of the Navy's FORCENet follows the International Standardization Organization (ISO) layered approach but in three main layers. It is the Navy's intent that information assurance, quality of service, and Human Systems Integration activities penetrate all three layers of the reference model. A plan to evaluate and mitigate risks to network enterprises must consider the network's layer abstractions. For the network's security software logic and mechanisms to operate correctly, it is important to know in which network layer abstraction a risk mitigating strategy will be defined and implemented.

NETWORK ENTERPRISE RISK MANAGEMENT

That adversaries are preparing to deny U.S. and allied forces free access to information supporting superiority in military operations is sound judgment supported by much evidence. Along with possible organized (on a national or sovereign scale) efforts to deny the U.S. military access to their information, many independent actors exist with an agenda and motivations not necessarily aligned with any cause who relish the

challenge of breaking into networks containing high value information; not the least of these is the U.S. military's network systems. For this reason, DoD has mandated that a major part of the development and operation of information system networks is the requirement for a robust information security program, primarily centered on Information Assurance (IA). IA is chartered to develop, test and implement measures to protect networks and information systems' assets while at the same time meeting the sometimes-conflicting objective of maintaining maximum network accessibility to the war fighter who needs it; many times under hostile conditions or harsh environments.

As the expertise of the threat in being able to "hack" into networks continues to grow at an ever increasing pace, the costs of countering that threat can skyrocket as well. The complexity of the software programs and architecture designed to mitigate the risks of today and to anticipate the risks of tomorrow brings with it higher costs in technology acquisition, costs of training operators in its installation and operation, the engineering costs of design and testing to ensure the right countermeasures have been acquired and applied, and the costs of vigilance in monitoring the network for intrusion. As Bruce Schneider said in CIO magazine concerning network security: "I'm here to tell you it's not about the technology" (Schneider, 2001). Since it is increasingly difficult for countermeasure technology to keep up, he advocates a program of continuous monitoring of the network's operation. With the responsibilities of normal watch standing duties, the added monitoring of network operations places added burden on manpower costs, both real and opportunity.

To be able to mitigate risk to the operations of a local network or an enterprise system of systems and achieve operational or strategic goals, identified risks need to be assessed to make the decision whether it is worth the cost in funding or opportunity to plan and implement a mitigation strategy for that risk. The answer to the question "What is this mitigation strategy protecting?" has a direct effect on the mitigation strategy employed. For risks of little or no impact no matter the likelihood of occurrence, the mitigation strategy may be one of accepting the risk as is. Implementation of security requirements that restrict functionality of a network incurs monetary as well as opportunity costs, life cycle costs, and some hidden or latent costs (such as stakeholder

costs in the future). If the system and its information that is protected have little impact on the success of achieving the desired effect, it might be prudent to reallocate that funding and technical solution elsewhere.

Network enterprise risk analysis is an important part of the implementation of a network's security posture as it overlaps with the IA program. Network enterprise risk management should be implemented at the beginning of a network system's lifecycle. The risk analysis and management process follows the steps of general risk management processes for safety, program, operational, and enterprise risks in organizations. Unique to network risk management is the concentration on an unpredictable threat who is motivated to exploit network vulnerabilities that the threat discovers for an ultimate goal of gaining something of value.

Drawing at once on the concepts of game theory and fault trees used in reliability analysis, attack trees can be useful in identifying and analyzing network vulnerabilities and the paths that can be exploited to gain access to the assets of the network. At the same time, they are useful in gaming the attributes of a threat that would make the threat more or less likely to make an attack on the network.

The risk management plan must take into account not only the threats, system vulnerabilities, impacts and mitigation implementation plans; but it must go one step beyond to determine how to architect the system for survivability and system recoverability. The network must be designed from well-considered requirements to resist, recognize and recover from an attack. The risk management plan must be mission-oriented. It must also be balanced, considering the costs of various risk mitigation and survivability design choices in terms of acquisition resources and in the effects of those choices on end-user functionality. The decisions made as a result of the risk mitigation and survivability planning and implementation drive the network architecture and design, and properly executed, result in an interoperable and networked system of systems and family of systems providing the war fighter with the right information at the right time, and easily operated programs and application to put ordnance on target and to keep the enemies' ordnance off us.

NETWORK SURVIVABILITY AND RESILIENCY

While risk analysis and management are designed to find and fix vulnerabilities that put the network at risk by the threat that exploits them with the intent to gain access to valuable information system assets, survivability is the attribute of a system that defines how it deals with an actual exploitation of network vulnerabilities that have remained after mitigation implementation. It is the architecting of a system before attack to respond to attack after other risk mitigation implemented plans have been activated to resist attack by mitigation plans that have reduced network vulnerability. In other words, survivability and resiliency are defense in depth for a network by designing the capability to continue action to resist and recover after an attack scenario. While it is vitally important to manage the risk to a network before attack and to make every effort to keep it from happening, a further defense mechanism and process needs to be in place in the event of an attack.

Survivability is scenario-driven, and defining survivability requirements with which to build a survivable network system is challenging. For this reason, the architect must look at the network's boundaries, the interface to other networks, and define where the line is drawn to resist attacks from threats that come in various ways with an array of capabilities. Once an attacker has penetrated a network, the architect must look at the capability of the system to adapt and recover while stopping the attacker's progression. Adaptability has to be built into a system on initial design. Unlike manned systems that can adapt with human intervention, network systems require adaptation in fractions of seconds, through complex software logic and must be able to do this automatically.

CONCLUSIONS

This thesis, (1) examines a network's architecture from the hardware aspect (topology) and software (layers and Service Oriented Architecture (SOA)) and how certain architectures create or mitigate vulnerabilities that could be exploited by threats,

and (2) develops a risk management process to enhance DoD Net-centric operations and the GIG architectural framework. The result is a comprehensive network enterprise risk management plan with the flexibility to adapt to a changing environment.

The second contention of the thesis is that the network enterprise needs to be architected with survivability and resiliency. A solid network risk management plan can inform the architects and engineers where a network's vulnerabilities exist so that survivability and resilience can be built into a network system designed to provide critical services in the face of an attack on the network.

There are risks associated with every endeavor. In the quest to develop an interoperable, interactive, and collaborative network enterprise across DoD that achieves DoD's strategic goal of information dominance against the adversary, a key ingredient in the success of that goal is to identify the risks to the network and develop a plan through knowledgeable assessment to mitigate the risks to an acceptable level. Doing this contributes greatly in allowing the network to provide the war fighters the information and capability they require to gain the edge in situational awareness, no matter the size or characterization of the mission. To shy away from the possibility of network attack by initiating uninformed security measures which unduly inhibit the network enterprise functionality, or to ignore the risk in an effort to meet budget targets, assures a less than satisfactory capability and acts as an impediment to reaching the ultimate goal of information dominance. Risk to the network enterprise must be dealt with up front by first designing the network for resiliency, second by constant vigilance to the changing environment at the boundaries/interfaces of the network, and third by building in an adaptability that learns from the attempted attacks as well as the successful ones, strengthening the network in every iteration. Proper employment of a rigorous network enterprise risk management plan supported by leadership delivers a network enterprise system that can deliver the goods of accurate, uncompromised, and available information when it is most needed.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I thank Dr. Edouard Kujawski for his time and mentoring throughout the research and writing of this thesis. I also thank Jean Johnson for her guidance and assistance in the development of this thesis. Additionally, I thank Mr. Bob Stephenson, CPF (N6T) and Mr. Jim Williams, CPF (N6T1) for providing the initial idea that blossomed into this thesis and for supporting the research in so many ways.

I would also like to thank Al Sargeant, Vice President & General Manager of Cubic Applications, Inc. for allowing me the flexibility to balance work and the Naval Postgraduate School through the duration of this course. In addition, many thanks to a great NPS Distance Learning Cohort (8), without whose support I would have faltered many times. Lastly, and most importantly, my eternal gratitude to my wife, Cindy, who gave me the encouragement to see this journey through to the end and the patience and forgiveness to let me do it in the first place.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

John G. Grimes, the Department of Defense Chief Information Officer states:

The security challenges of the 21st century are characterized by change and uncertainty. Operations vary widely and partners cannot be anticipated. However, we are confronting that uncertainty by becoming more agile. Greater levels of agility rest upon leveraging the power of information—the centerpiece of today’s Defense transformation to net-centric operations. (NCO). (DoD CIO, 2007, p. 1)

A. BACKGROUND

1. Information Technology Evolution

The information age brings new capability to the military by introducing software into the design of systems to run computers that provided control, automation and data manipulation, making these systems more capable. It is estimated that the contribution of software into the engineering effort of system design over the last decade has increased 30 to 70 percent (Maier & Rectin, 2002). Communications technologies benefit from the use of software by allowing the transmission of information in new forms; increasing the speed of delivery and the quantity of the data transmitted. Systems are tied together into networks so that data and programs can be shared between similar systems and across geographical boundaries to enhance the capability of the system and the war fighters who use those systems. However, this technology is applied in eclectic fashion to new systems development, so that when the systems are brought into production, they are equipped with the software available at the time they are developed. Out of this, systems and systems of systems are developed with differing characteristics (network architecture of hardware, software, and firmware, operating systems, applications, connectivity protocols, and use of the electro-magnetic spectrum) so that presently there are thousands of different programs running on different networks satisfying the requirements of a particularly stove-piped war fighting capability. In addition, the technology of computational power and networking is applied to the military’s business enterprise and to the collection and dissemination of intelligence data.

2. Information Technology Today

As information systems in the military grow in importance and capability, the services and DoD attempt to control the characterization of the systems' software and how systems operate through limited configuration control using standards like the Defense Information Infrastructure Common Operating Environment (DII/COE). This standard is designed to achieve a commonality between software components designed into systems to allow some form of configuration control and to allow interoperability between systems (Stewart 2006). However, the present information systems architecture in the Navy, and in DoD in general, is comprised of multiple networks serving stove-piped applications, which are further partitioned by functional category (business enterprise, combat systems, Command, Control, Communications, Computers, & Intelligence (C4I), logistics/supply and specialized intelligence gathering to name a few). The military recognizes now that information and easy access to that information is a key element in gaining an advantage over the enemy, and that the next frontier in warfare is the ability to leverage information system interoperability and to quickly turn data and information into knowledge superiority that results in the advantage over an adversary. Superior firepower is one thing, but the knowledge of when and where to apply it is another. To accomplish this mission and to achieve the capability of knowledge superiority, the military needs architecture for an integrated and interoperable information system of systems.

3. Future Vision of Information Technology

As the quote at the beginning of this section states, the leaders of DoD and the military services have clearly articulated their vision of information operations and the future strategy for military operations based on knowledge superiority. Computers and the automated processing capability inherent in them used to be seen as one of the technology tools in a tool set to increase the effectiveness of major weapons platforms and to increase capability in other aspects of operating, training, equipping, and communicating in the different warfare areas (NSA/CSS/GIG, 2008). Today, that vision has expanded to include information technology, processing and networking power into a

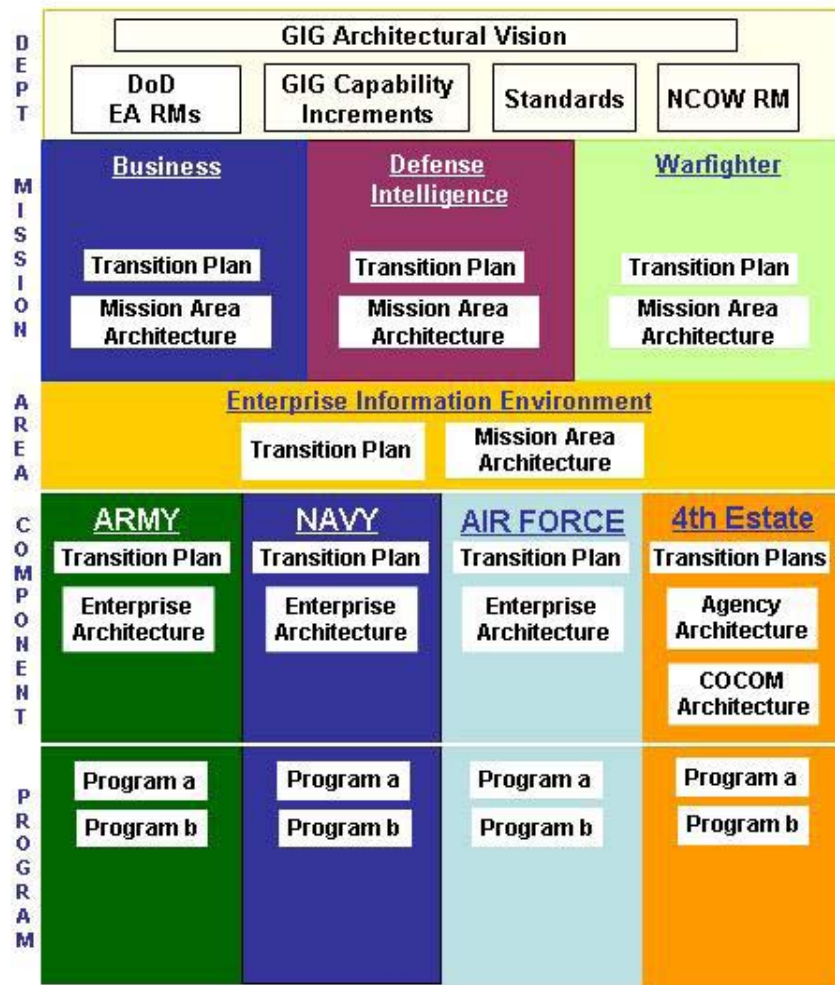
warfare area of its own, Cyber-warfare. Information and its collection, manipulation, distribution, use, and protection are considered vital to the future of warfare and are central to the defense strategy of the nation. Information systems are no longer considered to be stand-alone. They must be networked and interoperable; capable of sharing information with all authorized personnel and entities. Warfare and any military operation are now mandated to be net-centric.

To comply with the Secretary of Defense, the Chairman of the Joint Chiefs and the service Chiefs' vision, the DoD's Chief Information Officer formulated an architecture for the GIG and a pathway to take the military from the present day GIG to what he calls the Target GIG; a system of information capabilities gained through procedure and technology including doctrine, organization, training, material, leadership and education, personnel, and facilities (DOTMLPF) that provides an agile, dynamic, interoperable, and responsive system. Today's grid is sporadically networked along stove-piped structures of services, warfare areas, special capabilities, and partitioned organizations. While the networks are not an exact reflection of the chain of command under which they are governed, they do have somewhat of a hierarchical architecture to them. Each networked system uses its own technology base and is run in accordance with local procedures for the most part. There are over-arching rules and procedures emanating from organizations such as the Defense Information Systems Agency (DISA), National Security Agency (NSA), and individual service controllers as with Naval Network Warfare Command (NAVNETWARCOM).

4. Architectural Vision for Networked Information Systems

The target GIG architecture is designed to allow the users "to find and share the information they need, when they need it, in a form they can understand, use, and act on with confidence; and protects information from those who should not have it" (DoD CIO, 2007, p .7). The GIG technology is based on a SOA of loosely coupled repositories of services accessible to any node on the network that has access rights (what the CIO calls need to share). The technology draws from commercial technologies already developed to architect a system using Open Architecture, allowing a cost-effective way to design

and operate the systems throughout their life cycle and capitalizing on the reuse of software and firmware components. This architecture is the key enabler of Net-Centric Operations (NCO) and Net-Centric Warfare (NCW). Figure 1 shows a model of the architecture.



The GIG Federated Architectural Framework is the structure that ties the disparate architectures of the services together as they exist today.

Figure 1. GIG Federated Architecture (From: DoD CIO, 2007)

The ultimate goal of the GIG architecture is to move from a federated to enterprise architecture. To be federated means that individual programs are networked together through a tightly coupled framework. Enterprise, through the application of

SOA, means the systems are loosely coupled services networked on an architecture, which is agile and employs collaboration as its main ingredient of communication (DoD CIO, 2007).

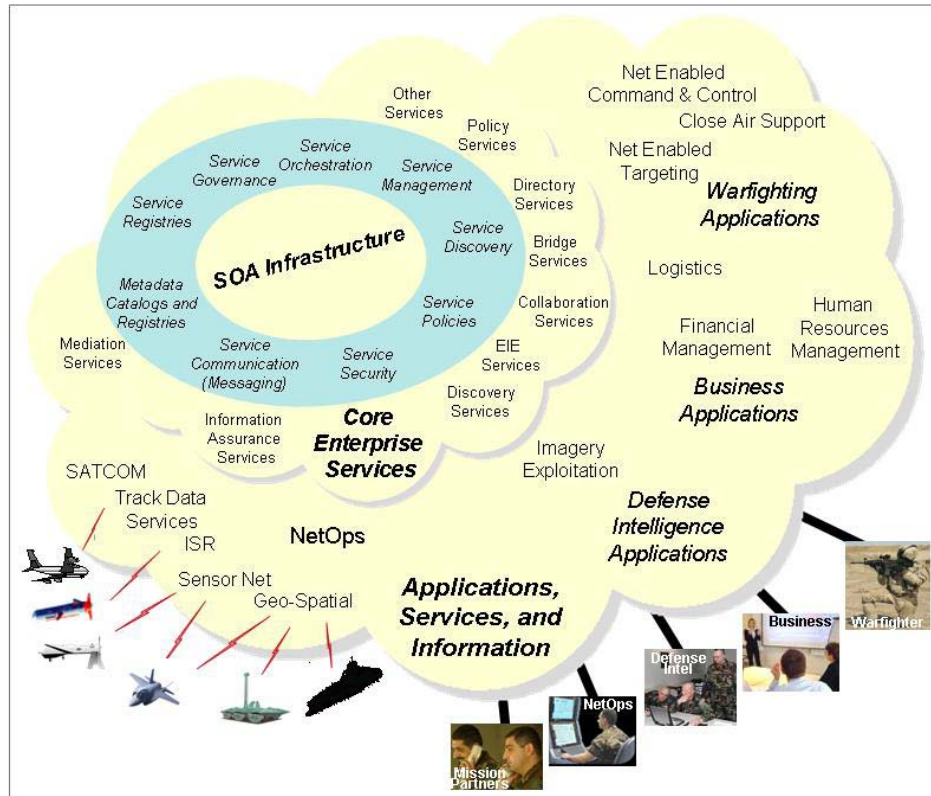
To achieve the vision of the DoD's target GIG, each service has an information technology initiative that falls in line with the architectural framework of the GIG, employing the principles of a distributed system built on a SOA. Standards are based on commercial standards boards as in Institute of Electrical and Electronic Engineers (IEEE), Internet Engineering Task Force (IETF), International Standardization Organization (ISO), American National Standards Institute (ANSI). Additional standards stem from service-specific initiatives including FORCENet for the Navy and Marine Corps, the Air Force Challenger program, LandWarNet as part of the Future Combat Systems for the Army, and Deep Water for the Coast Guard.

5. Challenges

a. Architecture

Many challenges face the achievement of a net-centric system of systems throughout DoD built on the target GIG architectural framework. The sheer size of the GIG technologically, financially, and procedurally is daunting (NSA/CSS/GIG 2008). Due to its sheer size and number of disparate networks linked together, security planning, implementation and coordination of effort across the services are difficult. Another obvious challenge is the coordination between the services as the development of a unified network architected in the GIG framework evolves. The service components may not be ready and willing to connect their individual network systems in synchronization with the target GIG objectives. Each service has individual goals they are trying to achieve, but for the GIG to be truly interoperable, there must be a consolidated set of objectives and a common approach to development controlled and monitored by the DoD agencies responsible for overseeing the development of the GIG. As can be seen in Figure 2, the set of services that reside in the GIG architecture are meant to be all-inclusive from all service components, tied together by SOA. The interoperability of the core services meets the CIO's goal of information sharing. Choosing a SOA is considered

to be a way of mitigating the risks associated with the interconnectivity of the complete set of services. However, the loose coupling of services through SOA allows connectivity and collaboration while keeping individual network interfaces less exposed to the vulnerabilities of those networks to which they are connected. Some disadvantages to this form of architecting core services connectivity are discussed in Chapter II.



SOA is a framework for achieving the CIO goal of information sharing between core services with an interconnectivity that promotes security.

Figure 2. GIG core Services and Underlying SOA Infrastructure (From: DoD CIO, 2007)

b. GAO Concerns

In a 2004 report, the U.S. Government Accountability Office (GAO) examined the process of GIG development and uncovered areas of concern (USGAO, 2004). GAO found the following.

- Identification and prioritization of technology investments was not yet articulated. With a system this large and complex, the financial decisions and the acquisition strategy have huge ramifications to the end product's ability to perform as desired. In addition, it is not clear how GIG technology investments impact other programs resources for development.
- There was not a clear understanding of how or who would enforce standards during development.
- Planning was lacking on how to deal with advancements in technology and how they would be incorporated (or not). Especially important here is what technology path to pursue as parallel technologies in hardware, software, protocols, applications and methods are developed. Which one would DoD choose to apply to the GIG? Since the GIG is based on open architecture, commercial products are an integral part of the system, and choosing the technology that prevails is important to the lifecycle costs and the development of other functionalities that depend on that product choice. Recall the DoD's choice of the Sony Betamax as the video cassette recorder for shipboard entertainment systems.
- A system this large makes it is difficult to evaluate the degree of enhancement to war fighting capability the GIG offers. In addition, the development of this capability takes some time, and as the national strategy and the environment change over time, a question of the ability to evaluate the new capabilities in light of new threats has not been articulated in the architectural framework.
- Network bandwidth has been a challenge to individual networks, and even with consolidation of some commercial services operating bands, it is going to continue to be a challenge as the size and the requirements for connectivity grow in the GIG. Through the GIG-BE (bandwidth expansion) program, the vision of the GIG is that it is agile to allocating bandwidth to the right entity that needs it in a temporal sense. However, the unknown is how much bandwidth the entire system requires and how it is obtained given the competing interests of national and international commercial enterprises and other Government organizations (such as the Department of Homeland Security).
- Protection of data within the current systems as well as the data generated during the development of the GIG has not been given the attention required. For instance, in the Core Enterprise Services layer of the GIG, "...Parts of the computing infrastructure are operated and maintained by commercial or government computing service providers (CSP) that provide managed services for hosting and maintaining enterprise services and applications..." (DoD CIO, 2007, p. 21). The GAO asked how the GIG developers assure current system owners (legacy and component owners) that their data are secure and remain so given the objective of the

GIG to broaden the sharing of information even with coalition partners who are not yet identified. Protection not only goes to the IA technology, but also to the procedures for safeguarding data, including the following.

- Who owns the data?
- Who has authority to release data?
- What is the plan if data is inadvertently or maliciously released to organizations or countries DoD to which it does not want it released?
- What is the impact on mission accomplishment?
- How is the impact determined?
- How to recover from that data being in the wrong hands.

c. Space and Naval Warfare Command Concerns

Other concerns and challenges in the development of a Net-Centric Warfare capability with a robust, agile and interoperable network have been expressed by service organizations, such as the Space and Naval Warfare (SPAWAR) Command and their systems centers responsible for the acquisition and development of Command, Control, Computer, and Communications, and Intelligence, Surveillance, and Reconnaissance systems (C4ISR) (Davis 2008; Anderson, Davis, & Green, 2008). Some of their concerns are the following.

- The **data protection policy** and a security architecture to protect data—a scheme for the prioritization of protection levels for data and how that affects the Multi-level security and cross domain solutions to the sharing of data. One plan for the protection of data is what SPAWAR calls a Data-centric Security Approach—prioritizing, partitioning, temporal value determination, data ownership, levels and need to access, storage and back-up requirement—are just a few of the elements of this plan.
- Establishing protections and procedures for the **supply chain management** of computer network components. This is especially important in the future development of Net-centric Operations, which are built on the concept of Open Architecture and the procurement of commercially developed and manufactured items. There needs to be a plan for how to ensure the level of quality of the procurement.
- **Configuration management** is important to the security of the networked systems to know what is running in each level of the architecture, and the plans for protection and recovery are valid for the known configuration. One of the challenges with service oriented architecture is the loose

coupling of the various services. Service providers have to have some standards of configuration control to assure the data users of the integrity of the service being queried by a user.

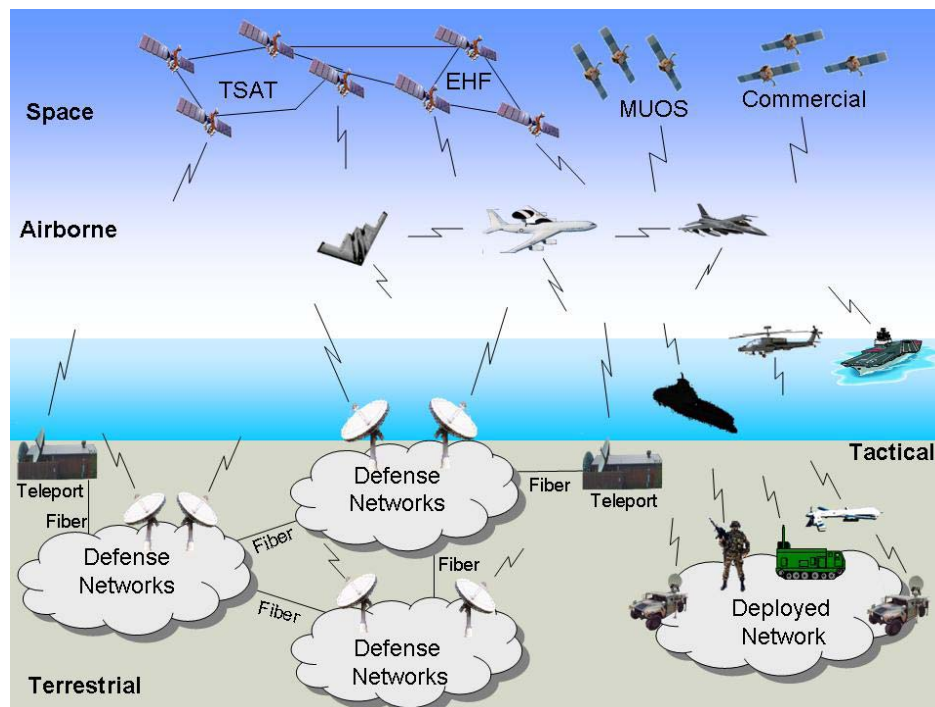
- The **GIG Information Assurance (IA)** infrastructure is built on five key elements listed below; however, net-centric operations and warfare need an information assurance policy and procedures for balancing the needs of the users with the levels of protection to meet user needs. In other words, maintaining a level of protection, which is affordable, enforceable, non-intrusive enough for mission accomplishment but strong enough to ensure mission accomplishment does not compromise degradation of the loss of the network or some of its components. Currently, the GIG IA infrastructure is defined by the following.
 - Transactional information protection
 - Distributed and automated digital policy enforcement
 - Defense against internal adversaries
 - Integrated security management, and
 - Embedded IA within enterprise components for a net-centric trust model
- For the current state of networked systems, whether interoperable, federated or stand alone, and for the target GIG and its components, the DoD **network enterprise risk management** plan should be robust, holistic, and structured, but should also be understandable and able to be applied at every aggregation and layer of the network system.

6. Service Networks Integration into the GIG

FORCENet is an example of how the services' architecture leads to the development of the target GIG when incorporated into the GIG system. Aligned with the architectural principles of the GIG, the Navy sees its FORCENet system as the integration of networks and communication with capabilities that are distributed and agile, able to make changes to configuration "on the fly." Network configuration adaptability allows a tailored network structure to be composed as needs are realized to meet the mission requirements in a distributed environment. The security mechanisms and Information Assurance program of FORCENet are envisioned to deliver information to the warrior that assures confidentiality, trust, integrity, availability, authentication and non-repudiation (inability to deny that correct information was received) (Stewart, 2006). FORCENet uses commercial standards in an open architecture philosophy, and uses the

same development principles as the GIG through the spiral model. This methodology is designed to be warrior-focused. Commercial standards and open architecture are used in the development of FORCENet to bring commonality to the systems, which comprise FORCENet and to use standards already in place that are working on commercial systems, avoiding the necessity to generate new standards through the development of proprietary software that is FORCENet specific. The purpose of designing FORCENet in a spiral development model is to transition stove-piped networks and programs from their programs of record to a net-centric configuration. The objective of the warrior-focused approach is to ensure the paradigm of “sensor to shooter;” the ability to get the complete picture prior to making a decision to engage (Hight, 2004).

Communication between services is based on the system presently built into the World Wide Web, the use of Extensible Markup Language (XML) and the Extensible Tactical C4I Framework (XTCF). Figure 3 shows a pictorial representation of the communications infrastructure as envisioned in the GIG.



The GIG communications architecture is based more on wireless connectivity than the Internet due to the military’s inherent mobility

Figure 3. Communications Infrastructure of the GIG (From: DoD CIO, 2007)

Communications technology from a physical reference entails several different modes, but the infrastructure is principally connected by fiber-optic cable and wireless technologies utilizing airborne and satellite relays. This setup of the infrastructure is not new for the military, but what is new is the architecture to combine these communications means into a cohesive network, which delivers accurate, timely, and sufficient information to meet the ultimate objectives of military strategy.

B. PURPOSE

1. After the Fact Risk Management Diminishes Network Capability

The purpose of this thesis is to investigate all aspects of a suitable network enterprise risk management plan in a GIG-like environment. Specifically, it provides the following.

- An examination of various network architectures and the advantages and disadvantages of different arrangements with regard to their ability to resist and recover from network intrusion with loss of confidentiality, integrity or availability of data, and functionality
- Risk and the risk management process; in particular, how operational and strategic risk management can be applied to operational and strategic global networked systems including the GIG and the services' network operations and to the mission success of a large organization such as the U.S. military.
- Specific risk management process models in use today with varying degrees of success by business and governmental organizations and how they can be applied to a risk management plan for NCO/NCW
- The definition of a survivable/resilient system and the necessity to include the attributes of survivability and resiliency into network designs and in the development of a risk management process/program.
- Network attributes that promote the protection of critical network resources from the disruption of network operations or the compromise of critical data. These attributes include defense in depth, fault tolerance, diversity and distribution, and redundancy and replication. As the Chief of Naval Operations has designated all his networks as critical, finding the attributes that work the best for the given network is a top priority.

- Bridge the gap between network risk management and architecting a network to meet the dual objectives of capability and security, with the ultimate goal of a global network of Joint military capabilities that can recover quickly in any environment or theater of operations and meet the war fighters' needs.

Why is the study and analysis of a network enterprise risk management plan vitally important? The complexity of the GIG and the services networks—FORCENet for one—make them vulnerable to attack on a number of fronts. If the networks provide the war fighter the information needed to win the battle, it is important to know where these vulnerabilities are and how to mitigate them so the vital information keeps flowing to the right places and individuals. It is postulated here that this risk management is best developed from the top down through the network enterprise operations to the nodes on that network and the services they provide and the users so that the plan is effectual end-to-end.

Risk can be dealt with in a number of different ways. Generally, risk can be eliminated, mitigated, transferred or avoided. While the IA engineers from NSA, DISA, and the services' systems commands have implemented many technical and process-oriented protections to the military's vast array of stove-piped and legacy networks, it is a common practice as prescribed by network operating procedure to avoid risk by isolating and terminating network operations that have been attacked, no matter what the level of the attack, the level of interruption to services, or amount of destruction to network data or programs. Risk management of the military's networks today is to a great extent comprised of information assurance efforts to examine and implement the best IA and protection technology tools, procedures and controls (countermeasures) to limit the possibility of intrusion from without and within that would cause degradation to the network or one of its nodes. Risk management planning appears to be somewhat reactionary, trying to plug the holes of vulnerability with technology or operational restrictions, or reorganization of resources and controls against known threats, and hoping that the technology guards against the unknown threat. Not much evidence exists that an examination of how the network countermeasures to resist attack are analyzed for their effects on network operations and the ability to bring information to the war fighter. In fact, the standard operating procedure appears to be a form of risk avoidance when an

intrusion is detected or a fault or failure is realized. The procedure is usually to “turn it off” as soon as a problem, real or imagined, is found. Growing concern exists among the war fighters about what might happen in the middle of a critical operation where the advantage in the fight is information and knowledge superiority, and that when a fault is detected in the network system, network system administrators and network management disable the network and deny the advantages of connectivity and information accessibility to the war fighter until the fault is located and fixed.

2. Summary of Purpose

This thesis investigates network enterprise risk management and determines what some of the likely risks are in operating a network as complex as the GIG and identify architectural tradeoffs available to improve network connectivity, functionality and security. DoD and services’ risk management plans in place today can be improved through the adoption of processes examining architecting a network for the following.

- Optimizing the often competing objectives of functionality and information protection
- Designed for survivability and resiliency to allow continued network connectivity even if limited

Principally, the network enterprise risk management plan can be enhanced to guide the management of network services and the formulation of policies and procedures that supports the war fighters in accomplishing their mission.

C. RESEARCH QUESTIONS

This thesis attempts to answer or provide some evidence to respond to the following questions concerning network enterprise risk management of the U.S. military’s network systems. The term networks means the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, imbedded processors and controllers” (Davis, 2008, p. 3).

- What considerations are important in developing and improving risk management planning and processes presently used by DoD and the military services for their information systems and networks on the global domain as Net-Centric Operations, Net-Centric Warfare, and Information Dominance now in the center of the nation's defense strategy?
- When and how should a robust network enterprise risk management program be implemented that supports the confidentiality, availability, integrity, reliability, and trustworthiness of the military's critical information resources and also acts as an enabler of mission success in the operational, strategic, and business processes domains?
- What are some of the architectural implications in the design and the process imperatives in the operation of networked information systems that make a global network system survivable and resilient to attack from hostile forces?
- Are there network risk management processes already in existence in the public domain supporting DoD's network enterprise risk management process to achieve a survivable and resilient enterprise network and support DoD in making risk assessments and decisions on the cost/benefit or value of the choices in implementing network security measures that ensure quality of service, information assurance, and meet the needs of the end user?

D. BENEFITS OF THIS STUDY

This study is intended to support improvements to DoD's and service component's Computer Network Operations/Computer Network Defense risk management process and support for the military's network management team as they examine risks to the present system of networks, which provide information to the warriors and to the network systems under development comprising the target GIG. This work encourages the incorporation of a network enterprise risk management approach when making decisions about acquisition, design, development, and operation of military networked systems.

E. SCOPE AND METHODOLOGY

The scope of the thesis is on the investigation of network risk management plans by other organizations and the applicability of some of the plans' elements to a generic network enterprise risk management for DoD, Joint, and Navy use. As part of the development of the above elements, the thesis investigates current models used in risk

assessments (CORAS, CRAMM, OCTAVE to name a few) and the possibility of adapting or developing a model for use as a decision tool in the military's network enterprise risk management process. The methodology entails the following.

- Research in literature and by selected interviews into present risk management processes in the military and in other organizations with complex networked systems (preferably architected using SOA)
- An evaluation of current risk management plans and models and an analysis of the models' application to the military network system
- An investigation of some architectural frameworks that might serve to improve the risk of operating network systems or serves to inform network designers of limitations, constraints, and assumptions arising in the design of networks when a proper assessment of network risk is conducted, looking at vulnerabilities and threats, the impact due to network degradation or loss, and the value of procedures to maximize network availability in a degraded state on mission accomplishment

THIS PAGE INTENTIONALLY LEFT BLANK

II. APPLICATION OF SYSTEMS ENGINEERING PRINCIPLES TO NETWORK ENTERPRISE ARCHITECTING

A. INTRODUCTION

This chapter discusses the architecture of a network from the hardware perspective of network topology and from the software perspective of open architecture and SOA. It examines the implications of managing the risks associated with network operation and how risk management is affected by the software architectural design and the arrangement of network components. The chapter's brief discussion of the different layers of a network system and their interaction with respect to network security and managing risks is covered more fully in Appendix A. Subsequent chapters examine the risks inherent in conducting computer network operations; how an organization might analyze the risks to network operations by identifying, assessing and managing risk both from a systems view of the network enterprise and the lower level view down to the client workstation level; and how process models that employ both qualitative and quantitative methods are useful in informing network designers and operators how to mitigate the risk of attack and protect the valuable assets of the network and the information in it. Commensurate with risk analysis is the study of how the survivability attributes, such as fault tolerance, of the network support the management of risk.

The architecture of a network is comprised of a number of elements. These include the topology of the network (arrangement of nodes and connections), the abstraction of information as it travels through a network, the standards used to assemble a network and the standards for packaging the information transiting a network, the type of components used for network node construction (switches, routers) and for transit paths (arcs) through the network (fiber-optic, twisted pair, wireless, satellite), how and where network components are acquired, the construction and control of the interfaces, the location of the network's information assets (data, programs), how and where the network connects to other networks or the Internet (gateways) as in a SOA, and the physical location of various components interacting with the physical environment (shipboard, desert,...).

Networks are architected in different arrangements to provide different capabilities while efficiently using available resources. The way a network is architected can introduce vulnerabilities through the make-up of the network components, by the way the components are connected, and by the methods employed, and the layer of the network where they are employed to provide protection for network and information assets. As network vulnerabilities are discovered and an assessment of the risks associated with those vulnerabilities is conducted, it is important to determine what network quality of service attributes the protection services and countermeasures (technological, procedural, or managerial) seek to secure or enhance through the protection of data and program resources, and how these attributes can be secured through innovative system design and network architecting. It is important in the development and operation of a network (as well as any system) to learn how vulnerabilities are created and how they are discovered. This information provides system developers with valuable experience to draw upon when developing follow-on systems. First, a brief discussion follows about the timing of commencing a risk analysis on a network and the importance of making risk analysis a continual process to take advantage of the feedback afforded by monitoring the success of mitigation efforts and by keeping the analysis current as the organizations objectives, technology and threats change over time.

It is the contention of this thesis that the identification, assessment, and management of network risks need to be done early in the system engineering cycle, in tandem with system concept definition. It is at this point when the Concept of Operations is the guide for determining the system's functions and for defining the system's requirements to meet the intended mission. Whether it is form from function or form driving function, the architectural foundation of the system must include an assessment of the systems' risk level from threats, and how the systems are architected to mitigate those risks or recover from an attack. The same is true for developing networks. All too often, a computer network and the interconnected information systems are a collection of systems

connected together for functionality, and only after the network has been intruded, are security measures integrated into the network system by means of software patches, which are put in place to mitigate another attack of the same or similar characteristics.

Before information systems became a ubiquitous commodity, system design built in safety as one of the design requirements, and system safety was required to meet strict specifications in critical control and operating systems where human and valuable property were at risk. With the advent of the revolution in information technology, and probably because of its rapid pace, system capability and the tremendous amount of applications that the new technology brought were given priority over safety and security considerations. Often, security was not just second on the priority list; it was almost ignored. Thus, with the systems already in place today, security tends to be more reactive; vulnerabilities are treated with patching to seal up the place in the program that has already been exploited (Davis, 2008). The same philosophy holds for the way many major commercial software products on the market are developed today. Security is covered by a library of software corrections to fix the vulnerabilities discovered by attackers. Vulnerability libraries keep expanding as new methods of malicious behavior from threat agents are discovered; usually, through a new attack on a legitimate system. At least the U.S. Government is trying to stay one step ahead though the Comprehensive National Cyber security Initiative (CNCI) (Germain, 2008). CNCI initiatives are an attempt to be proactive (in the true sense of the word, meaning action before consequences) by looking at establishing a front line of defense, developing cyber-counterintelligence plans, and shaping the future through cyber-supply chain management, deterrence, and defining cyber-security for critical infrastructures (Davis, 2008).

Networks are often created by connecting pre-existing stand-alone information systems together, often on an ad-hoc basis. With so many individual systems in the U.S. military inventory, the DoD has decided that the best architectural standard for connecting legacy systems together is through the method of SOA. One of the advantages of SOA is software reuse. Legacy systems in use today that were not developed to withstand the threat environment as it is today are networked in the new architecture to

avoid redeveloping the functionality these systems already provide. In addition to putting risk management in the systems engineering process from the beginning, the urge to ignore the security faults that legacy systems contribute to the network must be resisted. It is tempting to let resource constraints (as well as human nature's resistance to change) drive the decisions whether to take the additional step in architecting a system to resist and recover from attacks as well as architect the system to meet capability requirements. Additionally, while it may be at present, legacy systems' functionality will not be stand-alone in the future under the vision of SOA. The SOA, how it works and its advantages and disadvantages, is discussed later in this section. It is envisioned under SOA that legacy systems fit into the network architecture to connect their services (functionality) to the information grid. Being in an operational status in their life cycle, it is critical that a thorough risk analysis be done at the interfaces connecting these systems to the larger network. It is at these interfaces where a threat agent is most likely sought to penetrate and harm a legacy system's functionality. Through intelligent software architecture of the interfaces to legacy systems and the other Net-Centric Enterprise Services and applications, risk mitigation strategies can be implemented to provide protection to these assets and to the information and control required of them.

B. NETWORK CHARACTERISTICS

1. Attributes of a Network

There are as many ways to design and connect the components of a network as there are networks. No two are exactly alike. Networks can be characterized by the following.

- How they are physically or virtually (through software) hooked together called the topology.
- The basic function of the network (e.g., data storage and retrieval, command and control, business services, collaboration, supervisory control and data acquisition).
- The layer of abstraction of the communications between nodes in a network (data layer, network layer, session layer, presentation layer)
- The specifications of a network in memory capacity, processing power, signal latency, and bandwidth.

- The number and types of components comprising the network (switches or routers, central processors or embedded controllers) and the connecting devices used (Ethernet, synchronous optical network (SONET), optical fiber).
- The degree of accessibility or classification level of the network.
- The size of the network (Local Area Network, Wide Area network, Metropolitan Area Network) and its diameter (how many interconnections between end-to-end users).

The architecture of a network depends on the design and function of the individual components (nodes) and the way they are connected together (arcs of a network) to achieve an enhanced capability through their connectivity. Network node basic functional characteristics can be described with the following parameters when relaying packets or frames (wireless).

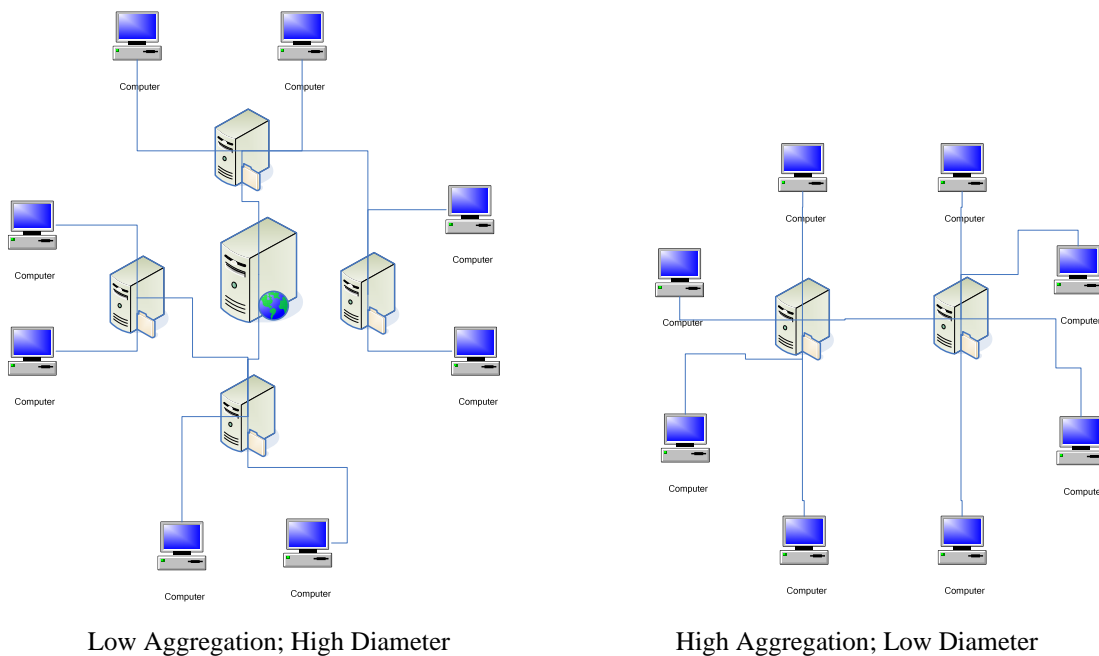
- Memory (buffer) capacity
- Processing speed (switching/relaying)
- The communications connection (arc in a nominal network) has the following performance parameter:
- Bandwidth (throughput rate)
- Interface processing speed (from Ethernet to fiber optic signals)

The goal in a network path is to get the signal, undistorted, through the network the quickest way under high bandwidth and low latency conditions. The parameters are constrained by signal latency, which is the time it takes for the signal to get from the source to the destination. This is determined by the number of nodes (switches), the switching time for each switch it has to transit, and the time it takes for the signal to travel through the communications cable. The bandwidth determines the amount of information that can be sent at once. Each time a signal passes through a node on the path between source and destination, it is called a “hop” in network terms. Since the travel time of light through the cable is a small fraction of the time for a switch to relay the signal between communication paths, the biggest contributor to latency is the number of hops the signal makes before it reaches its destination (Sterbenz, 2006).

A network diameter is the topographically farthest distance that a signal can go from source to destination. The “edge” of a computer network is comprised of those

nodes that do not act as relays for other signals. The number of hops a signal must take to get from edge to edge is a measure of the network's diameter. Thus, a network is bounded by its diameter. The Internet is described as unbounded because it is so large and it does not appear to have an edge (Sterbenz, 2006).

Aggregation in a network means connecting nodes to a central point. For a given number of nodes in a network, higher aggregation of the network means smaller diameter. More of the nodes are connected in a star pattern to a central routing mechanism as is shown in Figure 4.



Knowing the “shape” and number of connections in a network points the architect to vulnerabilities that can be corrected by changing the “shape” without sacrificing functionality.

Figure 4. Relationship between Diameter and Aggregation in a Network

Networks can be aggregated into three basic types: client-server, peer-to-peer, and a hybrid of these types. In the client-server arrangement, a component called the server controls the network communication between several “client computers” connected to the server, usually connected in a star topology. Peer-to-peer has no one component controlling communication, and the traffic management is done through the collaboration

of the “peers,” or active computers in the network, that are communicating. Client-server has an advantage of being able to more efficiently get signals through the network in an ordered pattern, depending on the network management program in the server, but the disadvantage in an intrusion scenario is that penetration and disruption of the server affects all the clients attached to that server. In wireless networks, transmission range and directional coverage are used to aggregate and control density. In high transmission wireless, everybody is connected to everybody. In low power wireless, nodes and overlays are used to control density and network diameter. Wireless network attributes take on a significant importance because of the GIG’s expanded use of wireless as opposed to the heavy land-line use in the Internet. DoD recognizes that with mobile forces, a significant amount of network connectivity is wireless-based (Sterbenz, 2006).

The scale of a network is the number of nodes and connections between nodes in a network. A network’s scale can be controlled by architecting the network into a hierarchy or by clustering segments of the network. In addition, the clustering controls system state as each cluster in the network can retain its own state separate from the other clusters. Clustering in a hierarchy can also control the amount of aggregation, thus limiting the effect of failure in a central node and not allowing it to affect the entire network or large portions of it. Clustering also supports the management of bandwidth allocation within the hierarchy’s sub-networks so that bandwidth through the larger network is managed when bandwidth is a controlled commodity of the network. Mesh networks (a topological arrangement discussed below that has the network nodes connected to every other network node I through its own arc) form natural clusters and can scale better than bus networks, allowing more versatility and adaptability in the network architecture. This also improves the network’s resiliency and recoverability after attack and network fault or failure (Sterbenz, 2006).

2. Network Quality of Service Attributes

The quality of service (QoS) attributes that need protection from malicious actors who would seek to disrupt operations are confidentiality, integrity, and availability (Davis, 2008). It is the goal of the network’s owners to ensure that the data, services, and

the control of critical operations are (1) available when and where they need them, (2) be unavailable to those that should not have them, and (3) be uncorrupted by those that should not have access to them so that the desired tactical, operational and strategic effects happen, and safety of personnel and systems is not compromised. Conducting a risk analysis of the network is vital to understanding how at risk these three attributes are, and whether or when they may be compromised because of system unreliability, accidental faulty operation, intentional intrusion, manipulation, or denial of network operations. The definitions of the three main QoS attributes are as follows.

- Confidentiality is the quality attribute that information is seen or given only to those authorized to see it. If someone unauthorized unintentionally or intentionally can gain access to the information, then confidentiality is compromised or lost.
- Integrity is the assurance that information received is the same information that was sent; nothing added, subtracted or altered. If data integrity is lost, information at the reception end sometimes seems ambiguous; however, ambiguity is often created by the sender and should not necessarily be attributed completely to a loss of network integrity. Information whose integrity has been compromised is difficult to detect unless there is a way to back up or compare the quality of the information received by information from another source, or by attaching a quality code (check sum) to the information sent.
- Availability is quantitatively defined as the percentage of time that the network system is operating as intended to produce the effects desired by the network owners and users (Hernandez, 2001).

In addition to these three attributes, non-repudiation (neither sender nor receiver can deny sending nor receiving what was sent or received) and authentication (verification of the identification of people and information) are important attributes to protect on networked systems.

C. NETWORK HARDWARE ARCHITECTING

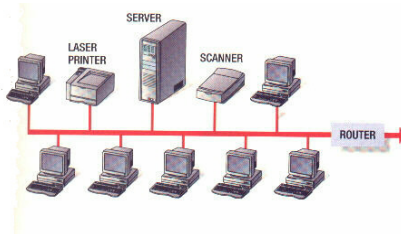
The topology of a network is the arrangement of how a network's components are connected, physically and logically through software. There are many considerations and motivations for choosing a particular topology for a network; cost and capability are probably among the preeminent. A network can take on a topological arrangement from its design and over time may take on another shape as the network evolves by added

technology, changing requirements, and not the least, by its addition and connection to other networks. Among the motivations for choosing a particular network topology, architecting it to protect its purpose and its contents and to contribute to the protection of the networks with which it is interoperable or loosely connected should be of the same importance as the capability it provides. No matter how capable the network and its component functions are or what contribution it makes to the larger network enterprise, if it is architected with vulnerabilities that can easily be exploited, any contribution to meeting the organization's objectives is most likely to become detrimental. A majority of the time, a compromised network can aid an attacker unknown to the network's owners until it is too late.

There are five basic types of network topologies; bus, star, ring, tree and mesh (Kioskea, 2009). While the pictorial representations of these arrangements look like their descriptions, the actual physical arrangement is created in the hardware used to make the connection and in the software program used in the component used to connect them together. While the basic topology of a network is the connection of components (as in a Local Area Network), the nodes of the network could be other networks, which are attached in the prescribed arrangement. These topologies are discussed below (images obtained from Google Pictures).

1. Bus Topology

In the bus topology, the components or nodes of the network are connected to a common bus known as the "backbone." It is the simplest organization of a network; each



component connected by communications line and their hardware adapters to the common bus. It is also vulnerable to degradation or failure should one of the components fail; in particular, a component that is attached to manage the traffic across the bus. While

the advantage of a bus is that it is easy to add components to the network, this makes it easy for an unwanted component to add itself to the bus and gain access to the authorized components.

2. Ring Topology

The computers in this topology are not necessarily arranged in a physical ring; however, they are connected by software that handles transactions between components



in a ring pattern, by handling component “broadcasts” or requests for service in order of where the component is located on the ring abstract. Information flows within this connection in one direction and each component has a turn to transmit or receive data in their order in the ring. The traffic management is usually handled by a program called “Token Ring” or fiber distributer data interface (FDDI). The FDDI architecture can provide a dual ring for added stability and network recovery. If one ring fails, the second ring picks up the communications management task. Under a dual ring technology with a concentrator (multiplexor to combine many signals into one), the individual components’ failures have less effect on the network performance than under a single or dual ring topology. Unlike a bus, the ring topology contains components in a tighter arrangement with more resistance to outside intrusion; however, the basic ring is vulnerable as failure of a component or one communication line to the ring causes the entire network to fail and cease communication. As mentioned, the dual ring arrangement offers recoverability capability. The time to establish the second ring would be an important specification depending on the service or data requirements of the network.

3. Star Topology

Star topology connects the components of network together by communications line to one central location called a hub. Traffic management and communications order

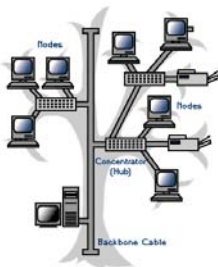


is maintained in the hub to send the communication from a source to a destination without involving the other members of the network who were not intended to receive the communication from the source. An increase in the sophistication of the hub device allows for more capability in traffic management and detection of stray or unwanted traffic. The hub could be merely a central collection and distribution point or a switch to control timing and priority of message delivery. A router, as the central point of the network, can

provide additional capability in the connection to other networks and as a firewall for incoming traffic. A router is a network hub with special capabilities to bridge to other networks. One advantage of the star topology is that the failure of one component or its communication link does not affect the rest of the network, unless, of course, the component that fails is the hub. Star topology also offers the shortest latency between nodes on the star; the latency time dependent mainly on switching speeds of the central hub. However, the importance of the hub in the network can make this component a single-point failure and therefore susceptible to attack.

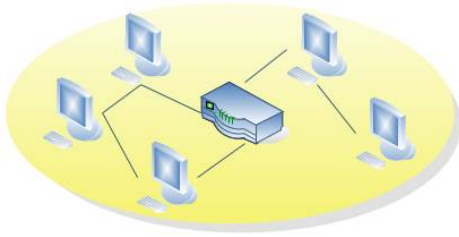
4. Tree Topology

Tree topology is a collection of star or ring topologies or individual components, which attach to a central bus via a concentrator component, with the concentrator/multiport hub that acts as a root for that branch. The concentrators can be connected in a hierarchical fashion with the root concentrator managing messages for an upstream concentrator as well as other individual components. This arrangement offers the advantages of the simplicity of a bus for the aggregation of the individual network arrangements and the protection of the star or a dual ring topology for each individual sub-network attached to the “tree.” There are multiple points on the tree that can be used to provide distinct levels of protection according to the level needed within the sub-network. Virtual Private Networks (VPN) or layer networks can be established within the tree, and the hierarchical arrangement of the concentrators can provide some defense in depth to critical components. Recovery techniques can be applied to the entire network or to the individual branches. It is vulnerable on the bus backbone to other networks attaching to the bus causing degradation to the rest of the network when one branch has a fault. It provides some fault tolerance when the fault is located inside a branch.



5. Mesh Topology

A mesh network connects each component to more than one other component via a dedicated communications channel. In a true mesh arrangement, all components are



connected to each other through a dedicated communications channel, so that no one component is controlling the communications of any other network component. As a network expands, if a true mesh topology were used, each component would need an increasing number of ports to connect to every other network node. In reality, the connections in a mesh are numerous but not total, and some components must have more connectivity than others to provide some type of traffic management or translation of information if some nodes process information differently than others. From the standpoint of vulnerability to intrusion, the mesh topology offers an architectural design with very good resilience in that a disconnection in one communication channel can be overcome by rerouting through a different path since all nodes are connected multiple ways. A mesh network can be complex to design and fabricate, as well as expensive with all the porting and channels. Deciding on the best mesh to maximize flexibility and resiliency and to maximize total network performance specifications of signal latency, bandwidth and computational power can turn into a multi-objective problem very quickly. As the diameter (number of nodes between end-to-end applications) of the mesh network increases, the shortest path between nodes quickly becomes constrained by individual bandwidth capabilities, switching delays, and communications link distances.

D. NETWORK SOFTWARE ARCHITECTING

To acquire a flexible, adaptable, and resilient global network, DoD had to make several system-of-systems (SoS) level architectural design decisions as it moved toward a net-centric philosophy of warfare. Two of the major decisions were to design networks under an open architecture computing environment and to build the global network to distribute, store, and operate on information in a SOA. This decision required the acquisition and incorporation of commercial off-the-shelf (COTS) technology into information systems and networks and was driven by the fact that to develop this technology in house would be too costly and untimely. Chapter V discusses survivability of a network. However, it is important to note, that unlike survivability as defined for

weapons platforms in battle situations, survivability of networks is protocol-based, not topology-based. Thus, it is the interaction between nodes that defines how the network interfaces are designed through software logic.

1. Open Architecture

a. Open Architecture Computing Environment (OACE)

The use of Open Architecture standards in developing information systems and networking them has been required by DoD and the Navy since 2004 (Naval Surface Warfare Center, 2004). The idea of open architecture is to use COTS products that meet common industry standards and to incorporate them into new and existing systems in a modular design. The Open Architecture Computing Environment (OACE) defines the key systems interfaces with commercial standards by industrial standards organizations.

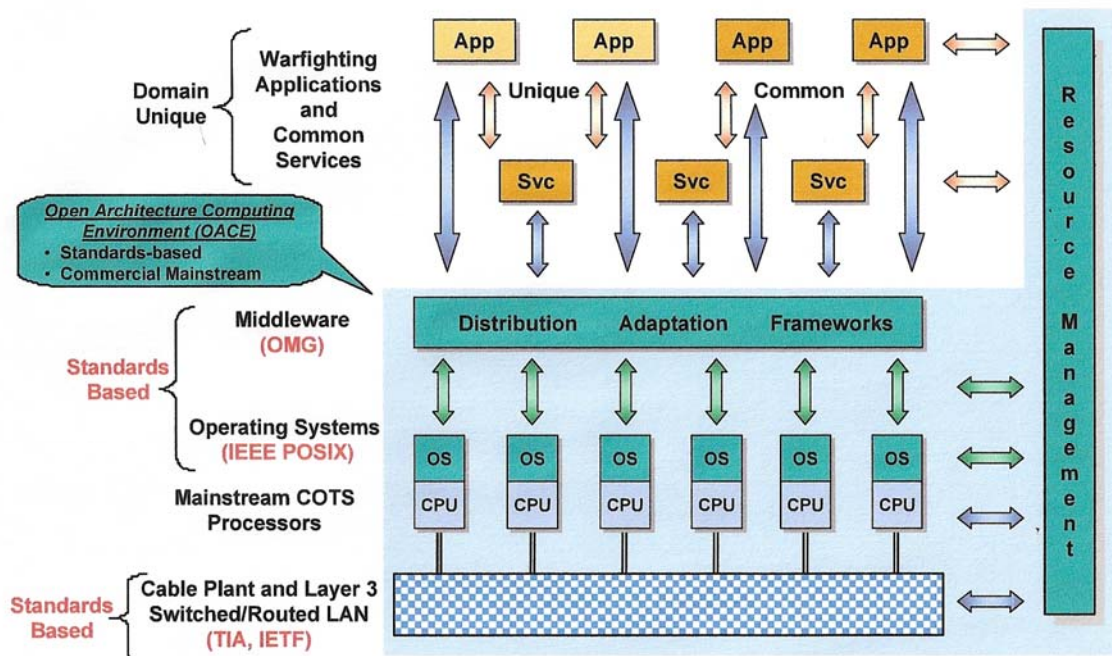
The OACE sets the standards of COTS hardware and software components and systems that can be used in the architecting information systems and networks. The standards, drawn from the DoD Joint Technical Architecture, promote user portability, or the ability to develop applications that interoperate with other applications and with a wide range of suppliers because they are engineered on the open standards for the following:

- Communications
- Abstraction of services
- Application Programmer Interfaces

The OACE is based on a reference architecture using a layered approach so that specific war fighting applications can ride on the layers and can interoperate and communicate with other mission-critical applications in a distributed environment. The standards in each layer are as follows and are shown in Figure 5.

- Applications: Java Programming, Java Community Process
- Language: American National Standards Institute (ANSI) programming C++

- Middleware: Object Management Group (OMG); Common Object Request Broker Architecture (CORBA), and Data Distribution Service (DDS)
- Network Operating System: POSIX Operating System
- Networks: Internet Engineering Task Force (IETF) for networks and protocols
- Physical Media: Telecommunications Industry Association (TIA) fiber optics.



Network layer abstractions allow the architect to focus on the form of the signal as it exists in that layer, enabling better architecting decisions.

Figure 5. OA Layered Approach (From: Naval Surface Warfare Center, 2004)

The range of functional applications built for the OACE are either integrated or federated. Integrated means commonality system-wide: resource sharing, enhanced recovery through redundancy. “The integrated approach enables mission flexibility and enhanced failure recovery through a high degree of redundancy delivered via operational resource sharing.” (NSWC, 2004, p. 12) Federated means unrestricted choice: maximum flexibility to meet unique requirements.

The OACE runs on the following layers, which mimic and are based on the four of the ISO layers.

- *Physical layer:* fiber optics carrying multi-mode messages has a wavelength and aperture. Physical security includes enclosures to provide shock, vibration, and other protections from environmental conditions.
- *Network layer:* connectivity, transfer, and support protocols. Connectivity is the data link layer providing logical connectivity (IEEE 802 and Ethernet). Transfer is the network layer (IP and routing instructions and QoS). Support protocols are the many session, presentation and application protocols for communication, file transfer, and e-mail.
- *Transport and sessions layer:* The network operating systems in this layer provide structure, priority, timing to comply with real-time operating systems to provide predictability. However, since the network's predictability is only as good as the most unpredictable component, the thrust of the operating system standards is based on the portability concept, a network operating system that can interface with other networks to which it is connected.

Two types of middleware are resident in this layer, adaptive and distribution middleware. Adaptive middleware isolates the application from the network hardware and the operating system. A Resource Manager supports computing capability (management to provide fault detection, tolerance, recovery) for computers that are input/output intensive, computing intensive, or memory intensive.

Four types of distribution middleware are included in the OACE: Distributed Objects protocol, Distributed Services protocol, Group-ordered Communications protocol, and Message-passing Interface for data parallel applications.

- Distributed Objects protocol supports data exchange by invoking methods on program application or data objects that can be remote. The distributed object protocols allowed by OACE are:
 - Distributed Component Object Model (DCOM) for non-real time business enterprise applications.
 - Java/Remote Method Invocation (RMI) soft real time for decision aids
 - Object Management Group's (OMG) CORBA—for soft real time command and control and hard real time sensors and weapons control

- Data Distribution Services (DDS) from OMG uses data-centric, publish/subscribe communications control for Command and Control and sensor/weapons control. Publish/subscribe distributes data to an application that declares itself a member. Data is distributed from anonymous servers to anonymous clients, as the information is not addressed for specific routing end-to-end.
- Group-ordered Communication protocol provides higher level of delivery guarantees; ordering messages to maintain consistency of state between replicated applications; detecting and recovering communications failures. The application can tell what communication was transferred before failure and what communication replication started after failure. Fault tolerance by application replication.
- Message Passing Interface (MPI) can be used for low/no-latency sensor control where real time control of data is important. Using data parallel techniques, this protocol is designed to handle parallel processing applications such as signal processing and for communication across a back plane of a massive parallel processor.

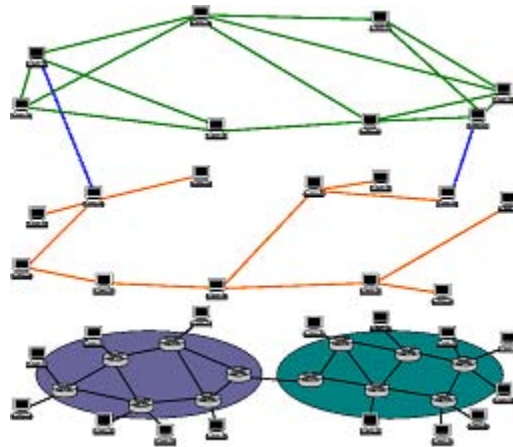
b. Vulnerability of Open Architecture

Open Architecture has the advantage of reducing development costs for new system software. The network architecture is composed in modular form from COTS products, which have the advantage of being already tested to a limited degree for reliability. However, the use of COTS introduces vulnerabilities that need to be examined for the potential of their exploitation by threats. In particular, commercial hardware and software has limited or no test and verification pedigree, and limited documentation inhibits optimum architectural design and the ability to determine exact reliability or develop certified and tested recovery procedures (Anderson & Hundley, 1998).

2. Overlay Networks

Overlay networks use software programs to draw on the topology of the lower physical layers and are defined by special procedures for linking certain nodes in a network together for special purposes. A VPN is an overlay of an existing topology in a physical network to provide security and privacy to certain nodes. The overlay or VPN can be scaled by physical characteristics of the communication signal or by authorization and authentication of new nodes requesting to become part of the VPN. An overlay VPN can also be controlled through the use of “Hash Tables,” which are a form of intrusion

tolerant multicast protocol. Hashing assigns a non-descriptive header on data transmitted over a network, so that intercepted data cannot be reconfigured to its original meaning. This form of addressing and describing data that flows through the network is mainly a device for database access when it is critical to have a high quality of service in confidentiality (Walker, 2008).



Overlay networks are an architecting technique that uses existing topology to provide the attributes of flexibility and adaptability. A virtual Private Network is an example of a network overlay.

Figure 6. Example of Network Overlay (From: Google Network Pictures, 2009)

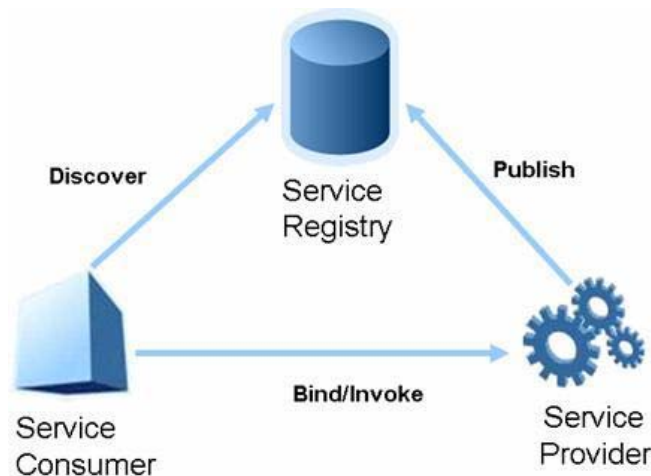
3. Service Oriented Architecture

a. Service Oriented Architecture Direction for the Military

DoD and the military services have several thousand applications residing on thousands of networks. Many of the applications are redundant, but they are accessed and executed by different means and in different languages. Rather than discarding all these capabilities from numerous programs that serve various functions and starting over to build functionality from scratch, DoD and the services are migrating their future network software architecture to a SOA (DoD GIG, 2007).

b. Service Oriented Architecture Definitions

Vijay Gehlot (Slide 6, 2009) paraphrases Thomas Erl's definition of service oriented architecture as a model in which functionality is decomposed into distinct units (services), which can be distributed over a network and can be combined together and reused to create business applications. These services communicate with each other by passing data from one service to another, or by coordinating an activity between two or more services. SOA draws on its predecessor concepts of distributed computing and modular programming. Technically, the communication between services is defined using a description language. The services have callable interfaces that are called upon to perform business processes. Each interaction is independent of each and every other interaction and the Internet protocols of the communicating devices. Since interfaces are platform independent, a client can use the service from any device using an operating system in any language (Gehlot, 2009). The communication independence between client and service is what produces a loose coupling between the interfaces of the network architecture. SOA is similar to the present architecture of Web-service, both of which use a service registry to allow a consumer of a service to discover available services through the Web Services Descriptive language (WSDL), and to access the service through an XML-base protocol called Simple Object Access Protocol (SOAP). In SOA, the service directory and service description are contained in one location and communicate under the Universal Description, Discovery and Integration (UDDI) language. Figure 7 is a simple picture of the SOA set-up.



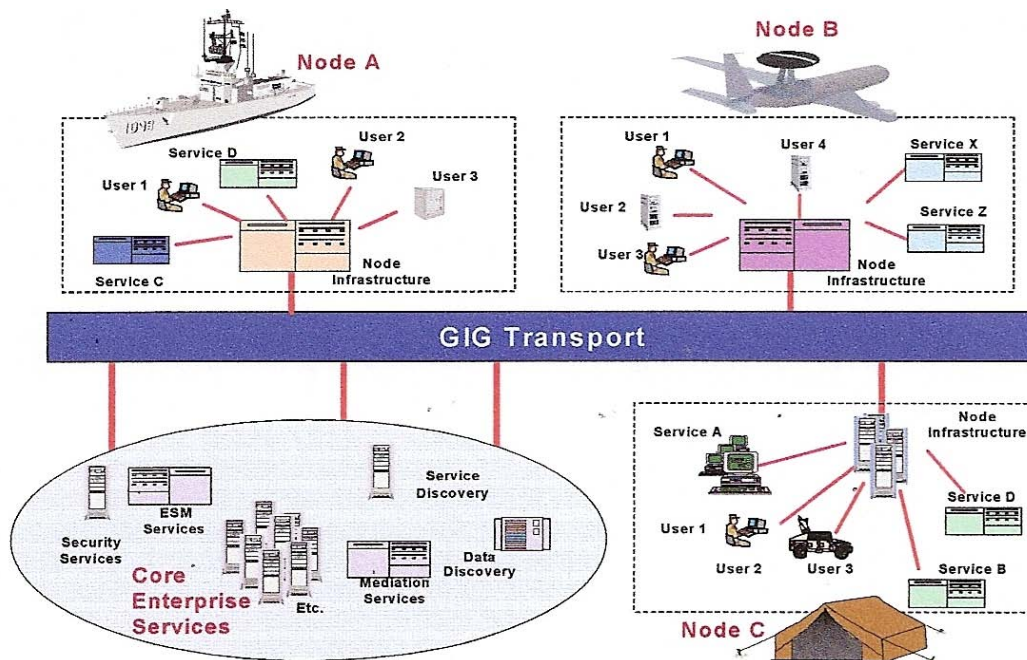
SOA discovers available services through a service registry, which decouples the service from the underlying operating system of the consumer, protecting that service from consumer malfunctions.

Figure 7. Service Oriented Architecture Arrangement (From: Geholt, 2009)

c. Distributing Services under Service Oriented Architecture

SOA is desired because of the savings on time and money by the reuse of existing software and services available through various programs. By structuring the enterprise network so that these services are accessible to any authorized user without the user having the program reside in the user's memory and rewritten in the user's language, these services can be distributed and used by anyone on any system platform and with any computer software language. When a service is needed to perform some operation, the architecture of the network is such that the user can discover the service desired, the service residing in some distributed location, and can call on the functionality of the service even though the service application may not be in the same software language as the user. The product that the user receives is in the presentation and display format of the user's workstation. The service does not need to know what program the user is running to provide the service requested. Through the technology of building an interface (SOA interfaces are ubiquitous) that can translate the language of the user's application with the language of the service's application or information resource of one kind or another, the user is able to access that service (if authorized and authenticated). Before it enters the network, requests for service or products from the service are wrapped in the

extensible markup language to describe what the information is so that when it arrives at the destination, the application can translate the data into a form it can use. The markup is usually done at the network enterprise services layer of the network (transport and sessions layer of the ISO model) where the middleware adds onto the information packets one of the middleware protocols discussed in the Open Architecture section above (e.g., distributed objects, distributed data services, group ordered communication, or data-parallel protocols for data-centric handling). Messages between nodes on a network are descriptive rather than instructive (loose coupling), and the messages must be extensible (changeable). Figure 8 is a graphical description of the way SOA is architected in the GIG, allowing the interconnectivity between units and services so that all can share in a common set of services.



SOA is envisioned to provide the connectivity between different warfare areas to promote “Jointness” and information sharing.

Figure 8. A Conception of SOA in Defense Applications (From: Gehlot, 2009)

d. Advantages of SOA

- Software reuse: transparent; neither knows what application the other is running. In this way, the network can be architected under software reuse. No new software programs need to be developed for the exchange of services except for the software in the middleware program that translates the service/data.
- Loose coupling between client and service. Coupling in simple terms is the reaction of one component given an action by another. Loose coupling between the client and the service or between two services means the actions taken by one program may be felt by the other program to which it is loosely coupled, which may or may not elicit a reaction. In tight coupling the reaction mimics the action. No coupling mean there is no reaction to the action from the originator.

Note: During the beginnings of software development, instructions to perform certain tasks called on subroutines to perform a service. The subroutine was part of the software program and was tightly coupled to the main programming. As program instructions continued to grow and as all services could not reside on one Central Processing Unit (CPU), a local network was established to put one application on a server that many clients could access and use. This was followed by object oriented programming, where the services were called upon by the network as objects (programs of a unique type that could be used and delivered as an entity) (Mahmoud, 2005). Object-oriented architecting of software contained strong links between service provider and user, and a change in user requirements usually meant a change in the object's programming to continue to be used by the new client. Under SOA, the trick is the design of the interface between service and user to loosely couple the two through software programming of the middleware interface to the network, allowing for changes in one end user or service not to affect the other end user or service. The language translation through the use of eXtensible Markup Language (XML) and later more sophisticated versions. Loose coupling allows for the rearrangement of the different services without affecting the users. This allows for flexibility and resiliency in networks (NSA/IAD, 2008).

- Testing new software applications can be done on the application itself, and not depend on the interface method except for the interface on the new program's end. This lessens the interruption of normal operations at other client sites and at the service site.

e. Challenges of Service Oriented Architecture

- Security across the architecture: While the loose coupling of the network connections between service requester and service provider gives the global architecture resilience in recovery from intrusion, it also means that the system, much the same as the Internet, is virtually unbounded and the number of users accessing services is unknown. Unnecessary requests for service or unauthorized service requests could go undetected using up valuable bandwidth and possibly compromising the confidentiality of information without the networks' owners discovering the loss until it is too late to recover.
- Testing in the SOA environment is complex because of the size of the global network and because of the complications of testing COTS products. Commercial documentation of software testing may be insufficient to uncover the faults or hidden programs of the code when applied to a military application. In addition, the loose coupling at the network's interfaces makes it difficult to discover a root cause for problems that span an interface. Software, whether commercial or proprietary to the organization, needs to have a formal process of quality control during testing to handle the unique aspects of software coding, and architecture to limit the existence of malfunctions and paths for intrusion. One such process that offers quality control in software design is Capability Maturity Model Integration (CMMI). Its use, while explicitly addressing quality control issues, puts the development of software one step ahead in limiting vulnerabilities in the software code and architecture. Vulnerability in software development and acquisition of COTS is a manifestation of its states, and controlling the states supports the control of vulnerabilities in the software (Chittister & Haines, 2006). Software testing is designed to evaluate the ability to control system states, but the complexity of software testing makes it virtually impossible to determine the ability to control all the states of the system.
- Managing metadata: networked, distributed services allow interception of information in packets while being routed without knowledge of either end user.
- The global aspects of SOA on the GIG means there are multiple connections of multiple types and it is difficult to manage the security across all those connections. As an unbounded network, there is limited governance from a global perspective. Governance is from multiple sources but do not translate easily across the loose coupling of the individual network's interfaces at routers and other gateways. It is difficult to monitor remote sites, especially if they are mobile and in a hostile theater. The diversity of multiple physical data transport devices and communication links (optical, wireless, satellite) while assisting in survivability through redundancy and diversity, causes problems with state

awareness in connecting networks. Interface connections, while loose, may have threat agents resident on the connected network that are unknown to the service requester. In addition, configuration control may be an insuperable task on a global scale, and configuration control loses some of its meaning when the point of SOA is to connect divergent applications across a transparent interface.

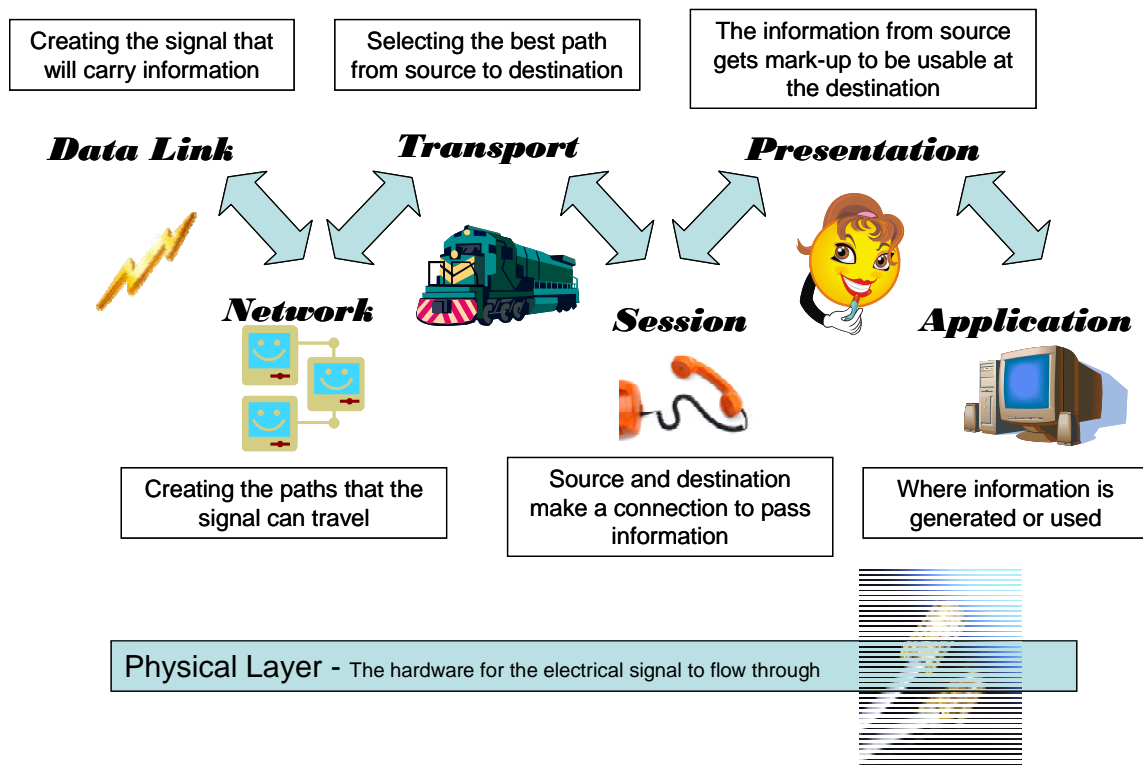
E. NETWORK ARCHITECTURAL VULNERABILITIES WITHIN NETWORK LAYERS

1. ISO Model

As discussed at the beginning of this chapter, a network is a complex organization of physical components and connecting devices arranged in a certain topology, signal paths, software logic controlling the signals, protocols which define how information is packaged, logic programs controlling the routing of the packets of information, packet addressing schemes to get the information from source to destination, software programs for determining who gets what information, mechanisms to keep packets from interfering with one another, the data and functionality contained in packets sent through the network, and a variety of other schemes for making the network operate correctly and perform the functions desired. The ISO has decomposed the operation of networks into seven layers in its OSI model. A plan to evaluate and mitigate risks to network enterprises must consider each abstraction layer. The seven layers are as follows.

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

Figure 9 is a graphical rendition created by the author of the ISO seven layer abstraction to focus on the interconnectivity of each layer and what function each layer is performing in the model.



An understanding of the form a signal or packet in each network layer abstraction supports architecting a resilient network at each layer.

Figure 9. Graphical Interpretation of Network Layer Abstractions

2. Vulnerabilities and Mitigating Strategies within the ISO Layers

Table 1 is a synopsis of an analysis of vulnerabilities in network architecture as seen through the information abstraction of the ISO's network layer definition. Appendix A provides an expansion on each of the layers in the table.

International Standardization Organization (ISO) Seven Layer Reference Model			
Layer	Quality of Service Attribute	Vulnerability	Mitigation Strategy
<i>Network abstraction</i>	<i>Attribute Information Assurance is trying to protect</i>	<i>What could go wrong</i>	<i>What can be done about it</i>
Application Services (e-mail, video stream, computation, collaboration)	Confidentiality, integrity	Fabrication, interception, and modification, of information inside firewalls and security management	Data replication, diversity, distribution and multiple sources of like services, multiple duplicated users.
Presentation Formatting, encryption, data compression	Integrity	Information markup in XML corrupted to intercept data, or incoming markup corrupted to deliver malicious program	Authentication, encryption, PKI, OS protection and virus data base updates, access control, distribution,
Session Setup and management of session	Integrity, non-repudiation	Session interrupted, or joined by unauthorized node capable of hijacking or eavesdropping on session	Authentication, access control, multicast, process and execution timing, intrusion detection, diversion, publish/subscribe schemes
Transport Complete messages and e2e recovery TCP	Availability	Intruder penetrates hole in VPN or layered network, or sets up unauthorized receipt permission at unauthorized node or hijacks intermediary node for DDoS	Behavior and pattern recognition, adaptive router reconfiguration, deception, secure protocols, middleware/box management, secure socket layers, VPN
Network Packet flow to establish connectivity between many links, provides basis for network management services IP	Availability, integrity	Network path management reconfigured for worst case routing or interception of packets on transparent internet	Intrusion detection, layered and mesh networks, , router access control and DNS server reverse lookup modification, IP repackaging (anti-spoof), distribution
Data Link Packets on one link	Availability, Confidentiality	Packets on open net are intercepted and modified or dropped	Packet verification and checking, redundancy
Physical Hardware and bit stream; cabling	Availability	Processor or memory chips from commercial source with secret code to reroute network traffic or intercept security management procedures. Electro-magnetic interference in unshielded systems at remote locations in foreign theater.	Redundancy, diversity, separation, physical access control, secure backplane

Each layer has its own contribution to providing a certain level of quality of service to the information flowing through the network.

Table 1. Network Vulnerability and Mitigating Strategies within Network Layers

F. SUMMARY: NETWORK ARCHITECTURAL CONSIDERATIONS IN MANAGING NETWORK RISK

A network can be characterized by its physical and its logical attributes. The hardware and software architecture of a network is a key factor in the vulnerabilities introduced into the design of a network system. When assessing the risk to a network, knowing the vulnerabilities that come from the architecture allows decisions to be made when considering alternative architectures to minimize the vulnerabilities to the assets of the network.

The topological arrangement of a network is the hardware architecture, and different topologies introduce different vulnerabilities. Mesh network architecture has the attribute that it offers the network superior resilience from attack, but these systems are costly and complex to set up. The software network management of a mesh network can be quite convoluted and hard to monitor the effectiveness of the management and security of the network. However, if the threat of attack against the value of the assets in this type of network is high, the cost and the complexity of design and installation may be worth it.

The GIG is a combination of many architectural topology arrangements, riding on the backbone of the DISA intranet bus. For this reason, a comprehensive enterprise risk management program has to consider the GIG architecture from the top down in aggregation and from the bottom up as each type of topology used in interconnecting networks affects the enterprise vulnerability picture.

In the risk assessment of the GIG's software architecture, the decision to use open architecture and to take advantage of the attributes of a SOA carries with it several area that can introduce vulnerabilities. Chief among these is the fact that Open Architecture and SOA is built from commercial products (COTS) that may be questionable as to the testing conducted before use in the military's network systems or whether there are hidden software programs or logic that can introduce unknown vulnerabilities that appear during network operation. Testing software, especially commercial, is problematic in that not all paths and software states can be tested within a reasonable amount of time or at a

reasonable cost. Quality control in the design of new software and integration of legacy and COTS software can provide some assurance that many of the hidden vulnerabilities are uncovered and corrected before that part of the network is put into operation.

THIS PAGE INTENTIONALLY LEFT BLANK

III. RISK MANAGEMENT OVERVIEW

A. INTRODUCTION

This chapter defines risk and the terms used in the DoD risk management process. The process is shown to result in the benefit of achieving the organization's objectives when used in a meaningful program that iterates the process throughout the lifecycle of the program or system under assessment. The next chapter focuses on the customizing the risk management process to a computer network, including local networks and a network enterprise system. Each chapter concludes with a summary of the reasons why it is time and money well spent to protect and secure the U. S. military's network assets and the information and functionality contained in it by formalizing a continuous network enterprise risk management program throughout the network enterprise life cycle.

B. RISK CATEGORIES AND DEFINITIONS

1. Risk

"Risk is the measure of the probability and severity of adverse effects" (Lowrance, 1976; Chittister & Haimes, 2006, p. 5). This classic statement of risk is simple but powerful. It can apply to a wide range of applications including the operation of any system and the conduct of any program. However, in applying this definition to any project or system, a major challenge is to develop a meaningful and valid measurement of risk, and deciding what is done with that measurement once it is obtained. There are different types of risk depending on what system or process on which the level of risk is being analyzed and at what level of the system or process is being analyzed.

- At the elementary level of a system or subsystem, the major concerns about risks to the system are from the standpoint of the system's safety and the ability to prevent harm to people or property.
- At the programmatic level, there are risks to the successful completion of a process, should that be the program's schedule, costs or level of performance. Risk and its measurement are key factors in the ultimate definition of the program's success.

- There are risks associated with the success of operations, including meeting the objective, having the desired effect, or maintaining an uninterrupted flow of accurate and reliable information that is vital to the operation's success.
- Risk at the strategic level affects decisions on allocation of resources, campaign plan and direction, manning levels, acquisitions to pursue, or policies to enforce.

a. Safety Risk

Looking at the risks to the safety and performance of systems, the U.S. Navy's Systems Commands define risk in NAVSEAINST 5000.8 (DoN, NSRMP, 2008) as "Risk is the potential for mishaps or other adverse variation in the cost, schedule or performance of a program or its products." In the operation of a system, the desired outcome is for the system to operate as it is designed. The risk comes from the likelihood of the system not operating as designed, and if that likelihood is realized, the consequences of degraded or failed performance in the safety to personnel and equipment including the people and property outside the boundaries of the system. The Navy's Operational Risk Management Instruction OPNAV 3500.39.B is a process for discovering and dealing with safety and hazard risks at the unit level (Kujawski, 2009). In his explanation of the correct operation of safety-critical computer systems, Neil Storey defines risk as " ... a combination of the frequency or probability of a specified hazardous event, and its consequence" (Storey, 1996, p. 60). Other definitions, which relate to risk when considering system safety, are as follows.

- A hazard (natural) or threat (human initiated) is an act or occurrence posing a potential of harm to a person or thing.
- An incident is the occurrence of a hazardous event which has the potential to cause harm under different circumstances.
- An accident is the unintended occurrence of an event or sequence of events that causes some measurable degradation or complete failure of a system or harm to people (Storey, 1996).

b. Financial and Program Risk

The Risk Management Guide for DoD Acquisition, 6th Edition (DoD RMG, 2006) and the Naval Systems Commands Instruction NAVSEAINST 5000.8 (DoN, NSRMP, 2008) both look at risks to a program; financial, schedule, and personnel that would inhibit a program from meeting key objectives in those areas. Program

managers are directed in those instructions to determine what might threaten the program's schedule, budget, or personnel from performing as required to meet objectives, and to weigh the probability of those inhibitors against the consequences to the program should they occur. Armed with that knowledge, a program manager can then develop a plan to decrease the probability of the unwanted events causing consequences unacceptable to the program. The guide defines risk by the following statement: "Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints." Program risks have three components.

- A root cause (yet to manifest itself), which, if eliminated or corrected, would prevent a potential consequence from occurring
- A probability (or likelihood) assessed at the present time of that future root cause occurring
- The consequence (or effect) of that future occurrence.

A root cause is the most basic reason for the presence of a risk. Accordingly, risks should be tied to root causes and their effects (DoD RMG, 2006, p. 1).

c. Operational Risk

Looking at risk from an operational level, Bilal Ayyub, (2003, p. 35) says that risk can be framed in the context of a scenario or event as the occurrence likelihood and occurrence consequences of an event. It is also the potential for loss or reward resulting from exposure to a hazard that if realized would result in an outcome of some measurable significance on a defined population of people and machines. Risk is measured by defining the components of the risk, measuring the chance or probability and measuring the potential negative or positive rewards or benefits (Ayyub, 2003). Ayyab is talking about both opportunity and adverse risk.

In the military setting, operational risk is encountered on a constant basis from the theater commander to the unit commander; only the level of the risk to operations differs at the echelon of command to which it applies. At the Combatant Commander level, risk of mission success or failure is considered when determining courses of action. In the doctrine of Effects Based Approach to Operations (EBAO)

[Commander's Handbook for an Effects-Based Approach to Joint Operations], the mission objective is to achieve an effect, or a change of system state of the adversary to what the Combatant Commander desires. Courses of Action (COA) are considered to achieve the effect desired, and each COA carries a probability that the action does not achieve the effect desired; an operational risk resulting in a consequence. An additional risk to operations from the EBAO approach is the risk that actions result in unintended consequences. "One will always encounter unintended effects, both good and bad, and those that extend beyond objective accomplishment. Improving awareness can help anticipate many outcomes and mitigate the impact of unintended negative effects" (Hunerwadel, 2006, p. 1). Conversely, a military adversary is also trying to achieve an effect on U.S. forces. The operational risk comes from the threat of enemy action, and the consequences if the threat should become reality. The military commander must consider what motivates the enemy to act, what the action is, what can be done to decrease or mitigate his forces vulnerability, and what the consequences are if the threatened action happens. This type of analysis is directly applicable to the way the risks to a computer network should be handled as is shown in the subsequent chapters.

d. Enterprise Risk

By the very nature of an enterprise being an integration of several systems (system of systems or family of systems) integrated and interoperable to some extent to achieve a common objective and produce the desired effects, risk to the enterprise takes on a holistic perspective (Haimes, 2007). Risks, or the likelihood of occurrences that would hinder desired outcomes that achieve the ultimate strategic goals of the enterprise, can come from external or internal sources and can be directed at multiple objectives such as finance, people, processes, and operational events. Dealing with enterprise risk requires common enterprise understanding, strategic communication planning, cross-enterprise alignment and sound understanding of the evolving environment (Kujawski, 2009).

2. Risk Analysis

Risk analysis is a process and practices to identify and assess risk. Risk analysis is designed to answer the questions of what could go wrong, how likely is it that it would, and what would be the consequences if it happened (Haimes, 2007; Blanchard & Fabrycky, 2006).

a. Risk Identification

The identification of risk is the process of ascertaining what could go wrong. Sources of risk can come from natural or man-made hazards, from unintentional incidents or accidents, from unreliable hardware components or software programs, from software that has been unintentionally or intentionally designed with flaws or faults, and from individuals or organizations (cultural or political) who desire to tamper with and disturb or destroy system effectiveness. Identifying risks of parties intent on harming a system requires matching the threat from these parties with the vulnerable set of system states that the threat can exploit. In particular:

- Threats and threat agents are entities with the motivation and the capability to cause system disruption, harm or failure. A threat is an event that has not happened but has a chance of happening; thus, a probability of occurrence is associated with the threat.
- Vulnerability is the degree of exposure and number of weaknesses in the system a threat could exploit. Yacov Haimes and Clyde Chittister (2006) further define vulnerability in software engineering as “...the manifestation of inherent states of a system that can be exploited or otherwise adversely affected...” The authors also say that to be able to control system states implies an ability to control vulnerability. For the threat to exploit the vulnerability, the threat needs to discover the vulnerability and when the optimum time to exploit the vulnerability would be to achieve the effect the threat desires.

b. Risk Assessment

Risk assessment is a combination of risk identification, likelihood, and the associated consequences (Haimes, 2007). Assessment of risk probably involves the application of processes and methodologies, often through the use of process models, mathematical formulations or simulation, to quantify risk elements and prioritize them for when and how to deal with them. Quantification of the impact relies on the assignment of

probability outcomes or values to the effect on the system that a threat capability, intention, and the threat's progress (again a temporal attribute) at completing the intended threat objective. The combination of the probability of the likelihood that a threat exploits a vulnerable system element and the impact that could happen quantifies the risk to a system for a given scenario. A prioritized list can thereby be generated. Risk quantification is a difficult concept to grasp let alone quantify into a metric.

3. Risk Management

Risk management involves the determination of what should be done about the risks identified. Risk management is the process of making management decisions, implementing the decisions (take action) based on risk assessment, controlling the identified risks and tracking the results of actions taken. Follow-up is equally important and involves taking further action based on the effectiveness of the initial actions, and continuing to monitor the environment, looking for changes to the environment that would change or change the course of action as the level of risk changes. Once it is determined what could go wrong, how likely, and the impact, it is then incumbent on the analyst to discern what can be done about it, what trade-offs can be made to decrease risk, and what effect the decisions to take actions to improve the measure of risk have on the future operation of the system (Haimes, 2007). Depending upon the degree of risk and the organization's tolerance of risks, coupled with the importance of accomplishing a given objective, the organization's action on the risk assessment yields the strategy to deal with risk elements by avoiding, accepting, transferring or mitigating the risk. The subcategories of managing risk, defined below, are the steps in the process for handling identified risks. These categories are mostly aligned with the DoD's definitions and processes for risk management, but some go into greater detail than the DoD Risk Management Guide (DoD RMG, 2006).

a. Risk Mitigation Planning

Planning for risk mitigation is the activity of examining courses of action that decrease or eliminate a threat posing a risk; patching or eliminating system or program vulnerability threat could exploit; or changing the importance of accomplishing

desired objectives to decrease impact or change the consequences if a risk becomes a reality. Mitigation can be accomplished through technological means or process and procedures (e.g., system operating rules, personnel selection and training) (DoD RMG, 2006).

b. Risk Mitigation Implementation and Plan of Action

Risk management does not end with the collection of ideas of what can be done with the risks identified and assessed. The decision makers must decide and act on the priorities established and implement their actions. Part of the decision-making process must be an evaluation of what effect the decisions have on the future operation of the system and what new exposures might be created because of their actions (DoD RMG, 2006).

c. Risk Management Plan Tracking

The effects of the actions to implement must be monitored to see if the goal was achieved, or if modifications need to be made to the implementation plan. In addition, any changes to system or program performance must be monitored as the environment surrounding the system changes. While monitoring the system response to the implemented plan, analysts should determine if the reaction is a positive or negative result of actually mitigating the identified risk or other changes (DoD RMG, 2006).

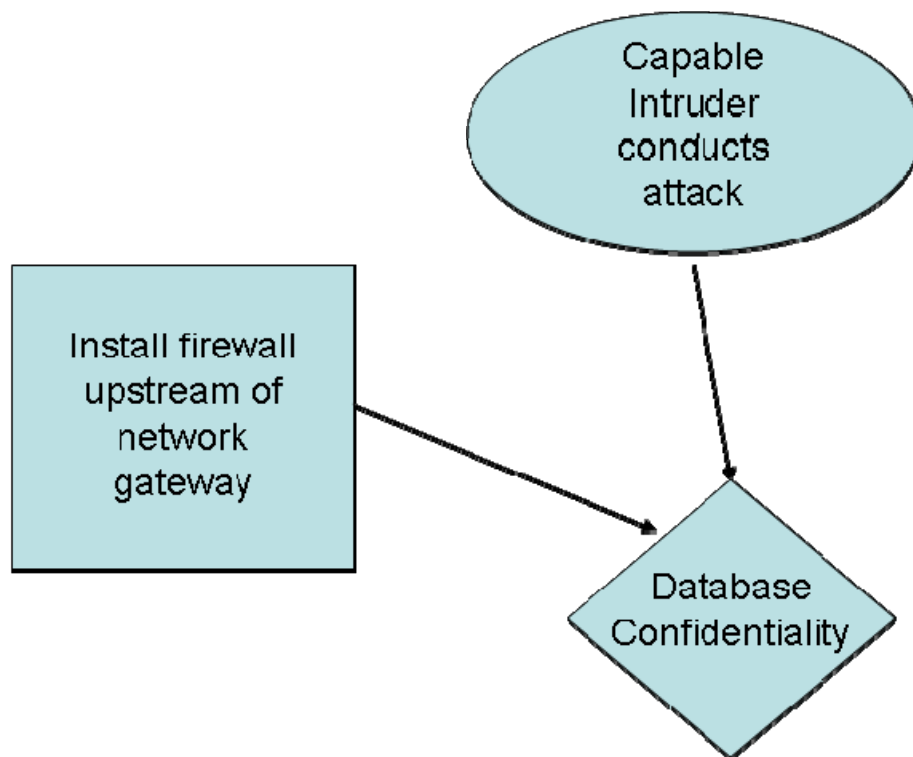
C. DECISION-MAKING PROCESS

1. Risk Factors/Influence

a. Influence

Understanding how risk affects the operation of an enterprise, which definitely encompasses probability and consequences, is fundamental to making good decisions in managing the risk. Part of that understanding comes from knowing what influences the decisions made and what influence those decisions have on subsequent outcomes. In turn, this motivates subsequent actions taken in response to the results of the first decisions. The experts in the field of risk analysis (Clemen & Reilly, 2001; Haimes, 2009) advocate using influence diagrams to aid in the visualization of the consequences

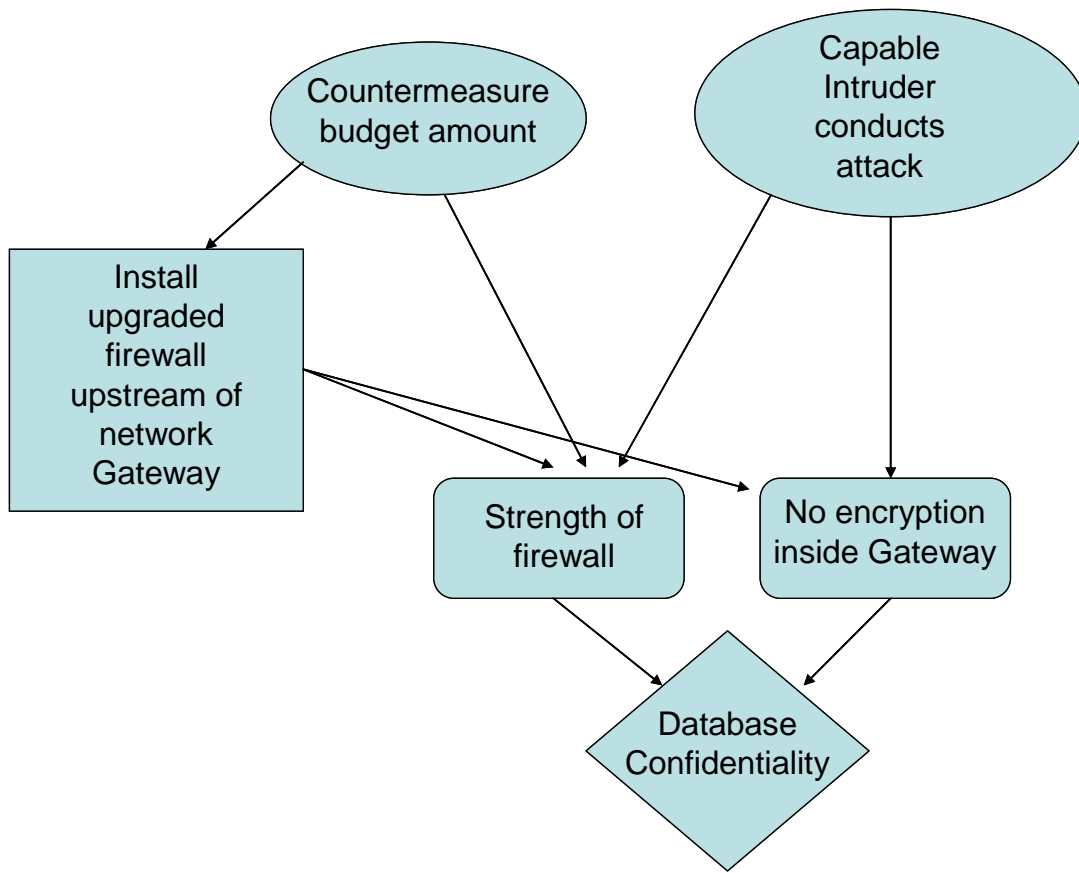
of making risky decisions. Influence diagrams graphically display the decisions, chance events and scenarios, and outcomes with arcs representing the direction of influence and sequence. An influence diagram helps the decision maker put decisions and alternatives in context and to visualize the factors that affect the desired outcome or effect. Influence diagrams can be used for both opportunity and adverse risk scenarios. When used to display decisions for risk management, the diagrams are mainly utilized to show the relationship between actions and outcomes as a result of adverse chance situations (risk) (Clemen and Reilly, 2001; Blanchard & Fabrycky, 2006). Figure 10 is an example of a simple, one-objective influence diagram on the decision whether to install a firewall in the network or not. Each action combined with an element of chance results in an outcome.



Decisions produce outcomes, and knowing the influences on the outcomes aids in making better decisions

Figure 10. Basic Influence Diagram on Risk to a Network

In the diagram, a rectangle represents a decision, a rounded rectangle represents an objective, an oval is a chance event, and a diamond is the final outcome, final consequence, or “overall satisfaction. The arrows are arcs representing either a sequence of events or relevance of an event. In the figure above, both arrows are sequential; a decision is made and a chance event may or may not happen. The outcome of whether database confidentiality is maintained or not, is determined by a decision/action and by the result of a chance event. The idea of actions and chance events coupled to yield an outcome is executed further in the next discussion. However, in the influence diagram, measures of probability of the chance event and the decision variables are not graphically shown. The idea of the diagram is to show the relationship between events of chance and actions. In a slightly more complex situation, an influence diagram could be used to show multiple chance events impacting on intermediate consequences, which arise out of the desire to meet two or more objectives. Figure 11 illustrates the decision whether to install an upgraded firewall upstream of the network’s gateway to the Internet is influenced by two chance events, the intruder again and the decision maker’s budget.



Knowing the influences causing a mind-set for making a certain decision supports better decision making

Figure 11. Multiple Objective Influence Diagram on Risk to a Network

Two intermediate objectives precede the outcome of whether database confidentiality would be compromised; stronger firewall protection, and because the firewall is on the Internet side, not requiring encryption within the network's LAN architecture to save on the budget and to increase data accessibility by authorized users. The figure shows how the chance event of the budget amount has relevance to the decision/action to install the upgraded firewall and to the intermediary consequences of stronger firewall protection and "no encryption inside gateway". The chance event of an intruder gaining access to the LAN has relevance to both intermediary objectives also.

The diagrams above are grossly simplified. It would be advantageous to carry the analysis one step further to diagram how the outcome of loss of confidentiality to the database would influence the desired effect of the network enterprise, e.g., the loss

of confidentiality on this network would give an adversary access to vital campaign plans and operations plans, which would have to be redone to gain the advantage. A thought to consider: the loss of the campaign plans, although highly unlikely because this particular network is isolated/disconnected from the Internet, would be catastrophic to an already deployed Army Division that is to follow those plans. This fact might increase the weight given to the influence of the intruder's attack and decrease the influence of the budget, causing a reallocation of dollars to this network and away from another.

b. Uncertainty

In his book on Risk Modeling, Assessment, and Management (3rd ed.), Yakov Haimes (2009, p. 158) explains how most decisions that involve a chance (probability) of the events or scenarios happening are based on maximizing the expected value of the outcomes' "payoffs." However, in risk management basing decisions on the expected value, or median, a set of outcomes resulting from action taken in the face of the probability of a set of scenarios is not necessarily a wise decision. In the section about the fallacy of expected value, Haimes makes the point that if decisions were based on the expected value of the outcome, systems would be constructed, ignoring the possibility of the low probability but highly catastrophic outcomes. His formulation for the way decisions should be made is to partition the probability distribution into segments and calculate the expected value in each segment. Even though the catastrophic events have a very low probability of occurrence, human behavior and preference tends to skew the integrated result toward actions, which protects the system against the catastrophic event more than if only the expected value of the total distribution were used. This method, called the Partitioned Multi-objective Risk Method, more realistically "conditions" the expectations of the decision maker, and allows for a practical decision conclusion in the face of risks to a system, especially considering the element of safety risk (Haimes, 2009).

As is the case in most real world systems, the probability of chance events is incomplete but some data is available and can be used to develop a probability distribution of the chance events. Two methods to estimate the distribution are the

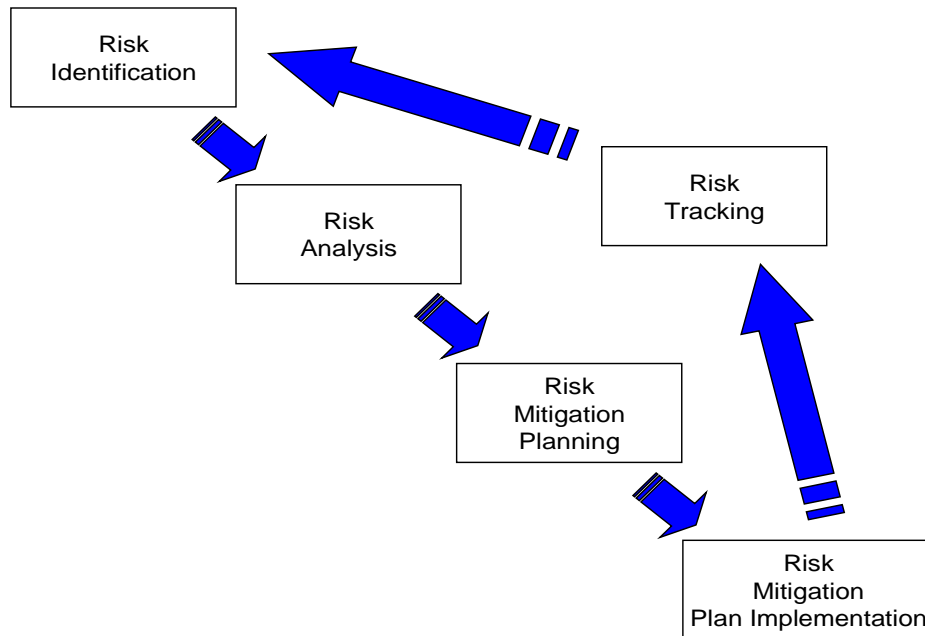
Fractile method by dissecting data into fractiles usually of 25%, 50%, 75%, and 100% and relating the outcomes to a fractile. Probability density and cumulative distribution functions can then be developed to give a probability to the chance events. The second method is to obtain expert advice on the lowest, most likely, and highest value of outcome. From this assessment, a triangle probability function is constructed with the base as the lowest and highest outcome values and the apex as the most likely. From the probability density and resultant cumulative distribution functions, probabilities of the set of outcomes are available to analyze against a decision to be made in light of the outcome (Haimes, 2009; Blanchard & Fabrycky, 2006).

To frame what is actually accomplished in a risk management process, the steps used by the DoD Risk Management Guide for Acquisition are used to illustrate how the process works in an actual very large organization for the management of programmatic risk.

D. THE DOD RISK MANAGEMENT PROCESS

The sixth edition (2006) of the DoD Risk Management Guide for Acquisition describes a generic process model for managing risk in acquisition programs. It is the DoD guide and template for other risk management schemes for processes other than acquisition and for the individual service components' plans for risk management within their service-related programs. The steps of the risk management guide closely follow the steps described above including risk identification, risk analysis, risk mitigation planning, implementation, and tracking, and is graphically shown in Figure 12. It also provides a planning guide for setting up a system of risk management in an acquisition program. The guide states that "DoD risk management is based on the principles that risk management must be forward-looking, structured, continuous, and informative. The key to successful risk management is early planning, resourcing, and aggressive execution" (DoD RMG, 2006, p. 22). The guide exhorts Program Managers to evaluate their programs in light of the risk to meeting cost, schedules and requirements. In fact, the

definition of risk in this guide is: “Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule and performance constraints” (DoD RMG, 2006, p. 1).



The basic process of managing risk is essentially the same for safety, finances, or operations. How it is applied depends in large part on the application..

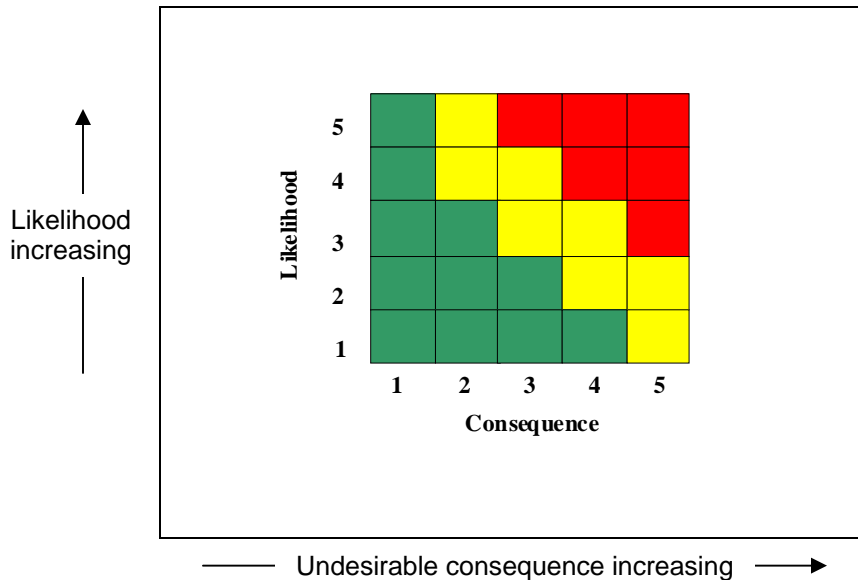
Figure 12. DoD Risk Management Process (From: DoD RMG, 2006)

1. DoD Risk Identification

The first step in DoD’s risk management process is risk identification. Risk identification is the activity that examines each element of the program to identify associated root causes, begin their documentation, and set the stage for their successful management. Risk identification begins as early as possible in successful programs and continues throughout the program with regular reviews and analyses of Technical Performance Measurements (TPMs), schedule, resource data, life-cycle cost information,... (DoD RMG, 2006, p. 7).

2. DoD Qualitative Risk Analysis

The next step in the DoD guide is risk analysis, a step performed much like the risk management models studied in the next chapter, where each risk element identified in step one is analyzed to assign it a likelihood of occurrence and an impact on cost, schedule, and/or performance. Figure 13 shows that the analysis is conducted qualitatively and the level of risk is reported on a Risk Reporting Matrix.



Qualitative risk assessment places the decision making in the right context; is it (the risk) something to be concerned about or not.

Figure 13. DoD Risk Reporting Matrix (From: DoD RMG, 2006)

The numbers for likelihood are matched to a table of probability of occurrence and enumeration of consequence is matched to a table that assigns the numbers 1 through 5 to schedule slip, cost overrun, or technical performance parameters. Interestingly, the technical performance parameters start with just meeting requirements and become progressively poorer. Also, included in performance risk is the program's management. While this is an important risk factor for a process such as acquisition, it is sometimes overlooked when evaluating risks to a system.

3. DoD Risk Mitigation Planning

Risk mitigation planning is the process of evaluating the results of the risk analysis and deciding on which risks need to be mitigated, how and when mitigation should be accomplished, and who is responsible. Risks that fall into the red blocks of the risk reporting matrix (in Figure 13) naturally have priority over risks that fall in the yellow region. Those risks in the green region most likely are considered to be acceptable risks, and no mitigation efforts are required up front. However, just because these risks are acceptable now, they still need to be tracked to ensure their likelihood or their impact does not change over the course of the program or change due to outside influencers. Once the risks have been prioritized, planning turns to ascertaining how to mitigate the most risky. The means of mitigation must be balanced against the costs of mitigation, not only the cost during acquisition and development, but also what impact a mitigation action has over the life cycle costs of the program or system. Mitigation actions might have implications on the technology required to mitigate the risk, and of course, the mitigation strategy has to examine and balance the opportunity cost that a mitigation strategy may have on system functionality (DoD RMG, 2006).

4. DoD Risk Mitigation Plan Implementation

Implementation is the process of putting the plan developed above into action. Implementation is the management function of communicating the plan to both action personnel and to the selected stakeholders who have a vested interest in the resulting new system requirements if the plan is implemented. Implementation is also the management function of assigning mitigation action responsibilities, and inspecting the progress and results of implementation. Finally, the implementation requires some type of reporting activity to keep program management aware of changes to a program and the effects those changes have on the program's cost or schedule. Justification for program cost increases or schedule changes can best be documented by relating them to the risks being mitigated and the consequence of not spending the time or money to mitigate an

identified risk. It also documents any changes to the performance parameters of the ultimate program's product because of changes to the system to mitigate a risk (DoD RMG, 2006).

5. Risk Tracking

As with any good management plan, after action is decided upon and taken, it is good practice to monitor the program or the system to see the result of the mitigation efforts. If the results are not what were expected, or conditions in the environment affecting program performance change, further actions or a change to current actions may be in order to keep the level of risk low, or to meet program objectives. The balance of the benefit of mitigating an identified risk must be weighed against the total cost of implementation and proper tracking of the results of mitigation actions supports or refutes the decisions made so that any non-working decisions can be changed. As the graphic of the process clearly indicates, risk management is not a once-through process. Tracking inevitably leads to the identification of other risks not uncovered in the first iteration of the process. Based on good systems engineering principles, the process is repeatable, in the case of this directive, throughout the acquisition cycle (DoD RMG, 2006).

E. SUMMARY

1. Benefits of the Risk Management Process

The rigorous application of a risk management process is an important weapon in the program manager's arsenal supporting activities and decisions leading to a successful program and a capable product. For instance, had the Future Combat Systems (FCS) program been able to quantify the risk that the integration of new networking technologies across such a wide array of hardware systems would have posed, the program directors might have been able to mitigate that risk by partitioning the disparate systems networks into manageable pieces. The consequences of that risk unmitigated are apparent in the fragmented status of the program today. As is evident in the FCS program, one of a program manager's important risk factors is the political environment surrounding a program, and equally important is the necessity to examine the level of risk contributed by that factor continually as the political environment changes.

2. Relating the Process to the Network Enterprise

The general methodology described above translates well to the analysis of risk and the implementation of mitigation strategies for information systems and computer networks. The risk process described above is related to programmatic risk in the Defense acquisition community, but as is shown in the next chapter, the basic steps for applying the process to programmatic risk are equally applicable to operational and enterprise risk encountered in local and enterprise networked systems. The basics of risk determination, probability of an event times the impact of that event, still hold true for the assessment of risk to a network.

3. Relating Benefits to Costs

To be able to mitigate risk to the operations of a local network or an enterprise system of systems and achieve operational or strategic goals, identified risks are assessed to make the decision whether it is worth the cost in funding or opportunity to plan and implement a mitigation strategy for that risk. The answer to the question “What is this mitigation strategy protecting?” directly affects the mitigation strategy employed. For risks of little or no impact, no matter the likelihood of occurrence, the mitigation strategy may be one of accepting the risk as is. Implementation of security requirements that restrict functionality of a network incur monetary as well as opportunity costs, life cycle costs, and some hidden or latent costs (such as stakeholder costs in the future). If the protected system and its information have little impact on the success of achieving the desired effect, it might be prudent to reallocate that funding and technical solution elsewhere.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ENTERPRISE NETWORK RISK MANAGEMENT

A. INTRODUCTION

Risk and the process of risk management as it applies to computer information systems and network enterprises is examined in detail in this section. While the basic definition of risk applies to networked systems and the management process framework is similar, information systems have unique attributes requiring a slightly different perspective on how to determine the level of risk to those systems. By connecting information systems into a network capable of sharing and collaboration, the number of possible failure paths and initiation points for intrusion to cause harm increases rapidly.

An analysis of the reliability of a network is important to the designers and architects of the system and is worthy of further study. To be thorough, the assessment of risk must integrate the risks and hazards associated with unreliability of equipment, accidental failures caused by equipment or people, and sabotage or attacks to obtain a true picture of the system's capability to support operational and strategic objectives. As reliability and human factors engineering generate key design criteria for a system designer, and since the contention is that risk covers all the categories above, the risk management process should include all those areas above and should be integrated with the determination of key performance parameters at the beginning of a system's life cycle, during concept definition and possibly before.

Information systems and network enterprises are at risk due to the following.

- Failure of hardware components, software faults and bugs, and network communication and signal failures
- Incorrect design, installation, arrangement of the interconnections between nodes on a network
- Human error by accident or faulty procedures
- Intentional invasion and destruction of hardware, software program logic and functionality, and network connectivity by entities intent on inhibiting correct network operation looking to steal or corrupt information

This thesis concentrates on examining risks to a network from the fourth source of risks listed above, intentional intrusion into a network with the purpose of causing harm. Recognizing and dealing with intentional acts designed to disable a network enterprise is challenging to understand fully. These challenges continue to grow as technology improves and gives the adversary more tools with which to intrude on network operations. However, the challenge must be confronted because the threat of network intrusions and disruptions continues to increase as the military relies more on networked systems to provide the edge in operations and strategy. The allocation of scarce monetary and human resources without a management plan is misdirected and may impede the purpose of the network in the first place. Installing technical network countermeasures or writing and enforcing procedures that affect the information flows and availability on the network supporting operations and strategy are without clear benefit and without robust risk management planning and implementation. Equally disastrous is when the risks are ignored or overlooked, allowing the adversary freedom to intrude and disrupt vital network functionality just at the time when it is most needed.

B. RISKS IN THE NETWORK ENVIRONMENT

The definition of the level of risk to computers and information systems from intentional intrusion can be defined in general terms as a function of the level of threat, the vulnerability of the information system and network, and the value of the system and information assets (Jones & Ashenden, 2005). Or put another way, risk is the result of a threat with adverse effects on a vulnerable system (Chittister & Haimes, 2006, p. 5). When no vulnerability exists to exploit, there is no probability that a threat damages network assets, and when a network's assets are not worth protecting, the measure of risk is low no matter what the probability is of a threat exploiting network vulnerabilities. More succinctly, risk from a threat to a computer network can be defined in the following equations as:

$$\text{Risk} = \text{Probability of Attack} \times \text{Impact of Attack} \quad (1)$$

$$\text{Probability of Attack} = \text{Probability that Threat will Exploit Vulnerability} \quad (2)$$

$$\text{Threat Probability} = \text{Threat Motivation and Threat Technical Capability} \quad (3)$$

$$\text{Threat Motivation} = \text{Enough Resources, Likelihood of Attack Success} \quad (4)$$

$$\text{Likelihood of Attack Success} = \text{Likelihood of Avoiding Detection and Impact} \quad (5)$$

(Ingoldby, 2009).

1. Safety Risk

Safety risk to a network is most often identified with networks that provide supervisory control and data acquisition, commonly called SCADA systems. SCADA systems are usually critical industrial, mechanical or electrical equipment operational control networks to monitor hardware system parameters and provide control signals to adjust inputs to get desired outputs. SCADA systems are networked to provide system managers information to change mechanical or electrical parameters and change system outputs. These networks are usually isolated and bounded by the industrial system they are controlling. However, if the network extends to a multipurpose computer that has access to the Internet, exploitation of these critical systems is possible from threats outside the system's boundary. For instance, if a control system on a ship supplies information to a system manager's computer also used for unclassified networking to other information systems off the ship, the control system may be vulnerable to attack from outside the ship. Since exploitation of a computer network vulnerability can come from a variety of sources, it is important to know if that adversity is from an intended act, an accident, or from a near miss (incident), as this information supports the decision-making process as it is applied to the management of risk.

2. Operational Risk

Operational risk is the threat to networked systems that provide information and functionality to accomplish a mission. Many activities on a network can be included in this definition. Civilian and military organizations want to achieve certain effects by the actions they perform, and the organization has short-term goals, which measure the effects achieved. Any network system contributing to the accomplishment of those goals

is at operational risk of failing to support the achievement of said goals. For instance, the network of UAV sensors to ground control stations that may be directly connected through a network to war fighters in the field that depends on the UAV intelligence and surveillance for targeting is at risk operationally as long as a way exists to exploit a vulnerability in the “sensor to shooter” network. Operational risk includes threats to a network that inhibit the network from achieving the desired effects supporting the goals of a unit or organization to which it belongs. Operational risk is a broader view of risk to a network than safety and program risk and must consider the integration of the people, processes and systems used in the attainment of those enterprise objectives and the external forces that would prohibit obtainment of those objectives (Kujawski, 2009).

3. Enterprise Risk

The aggregation of operational risks to a system or family of network systems can result in enterprise risk, which is the threat to the infrastructure or the long-term goals of an organization. It is important to understand that risk to an enterprise network is wrapped up in the nature of the integration and interoperability of the network’s components and sub-networks connected together. Enterprise risk is different than operational risk by the organizations’ assets and ideals that are possibly threatened and by the fact that the networks threatened by enterprise risk are most likely virtually unbounded much like the Internet. Unbounded networks were defined in Chapter I as a network where no one entity can know who is connected to the network at any one time or what connections are active in the vast array of paths between nodes that exist in the system. The action of exploitation in network enterprises usually takes place at the interfaces, and the network response to deterring or responding to an attack can depend on whether the systems at the interface are loosely or tightly coupled. Tight coupling offers a greater amount of control over the entire system, whereas loose coupling offers system resilience by containing the “infection” of an attack to one of the coupled systems and limiting the spread of the attack.

In a network enterprise, the ultimate goal is to achieve strategic information superiority. Enterprise risk is the probability that some threat agent has the desire and the capability to exploit the network enterprise, reducing or eliminating the information superiority of the enterprise, resulting in a consequence of varying severity to the enterprise's ability to achieve its strategic goal. As enterprise risk takes on a holistic perspective, so must the element of threat to the enterprise. The environment surrounding the network enterprise contains threats from other national interests, rogue players, evolving technologies, and internal people processes and policies (Kujawski, 2009).

C. RISK CONTROL IN A NETWORK

1. Balancing Security with Functionality is a Team Effort

Management of risk requires the application of risk controls on a system. Controls of risk to a program or system usually fall under the name of security. The method of controlling risk in any information system, and especially in the U.S. military's large inventory of information systems as they are networked together, is a balancing act between security technology and procedural implementation by system administrators and the desire for functionality by the users. The system administrators are charged with the security of the system, while providing usability that meets the needs of the mission. To accomplish this effectively, a dialogue between users and system administrators must be established so that security scheme and strategies can be aligned with the needs of the users, and the users must be trained in the network system vulnerabilities and how the vulnerabilities are being mitigated to lower the level of risk to the network. Without this dialogue, dealing with risk includes risk transfer or avoidance, which may unnecessarily limit the network functionality.

2. Controlling Risk is an Evolutionary Process Requiring Several Iterations

The controls put in place today do not necessarily guarantee effectiveness tomorrow. As the threat changes in capability and motivation, and as the network grows in size and changes in technical design, a robust risk management plan requires the constant evaluation of the risk controls in place and the requirement to change or improve

on their capability to lower the level of risk. Table 2 (Mulokey, 2009, p. 27) outlines some of the effects evolutionary change has on the security design and procedural implementation on network systems.

Evolutionary Changes	Effects on System Security
The user's tolerance for risk may change in response to changing world conditions, political considerations, or business priorities.	Stakeholders may require increased levels of assurance requiring tighter controls. Conversely, the greater need for the system's outputs may justify higher risk.
System components become obsolete.	Commercial off-the-shelf products no longer supported by vendors become vulnerable to attack
External sources can change the characteristics of their inputs to the system.	Anomalous responses to the changed inputs can degrade the system's availability or become an attack vector for sophisticated hackers.
Advances in technology instigate system modifications to improve efficiency.	Design changes may increase security or provide new vulnerabilities. Security analysis, design recommendations, and testing are key to assure security performance.
Workforce characteristics can change due to the retirement of experienced personnel.	Undocumented procedures can be lost when experienced personnel are replaced. Improved process documentation is needed to support training new personnel.

Risks to a network are always changing and must be reassessed frequently.

Table 2. Effects on Network Security due to Evolutionary Change (From: Mulokey, 2009)

D. RISK MANAGEMENT OF A GLOBAL NETWORK ENTERPRISE

1. Complexity of Network Risk Management for an Enterprise System

For an enterprise as complex and with such a breadth of coverage as the current and the target GIG, a process of risk management is a huge undertaking. The individual services' system of systems as exemplified in the Navy's FORCENet, Air Force's Challenger, and the Army's Future Combat Systems are in and of themselves expansive networks involving multiple physical infrastructures of connectivity and computational power, a vast array of software programs designed to control, operate and manage complex weapons platforms and inform, train, and command many thousands of specialized soldiers and sailors. Developing a system for risk management for the service components' information systems individually is problematic as the eclectic mix of current systems and their connectivity through thousands of different networks makes the

assessment of risk especially difficult. As is explored later, several studies on risk assessment have been or are being conducted on assessing risk within individual network operations. However, in the future, these individual networks are tied together so that war fighters can integrate intelligence and targeting data from selected sources to the weapons systems they are operating along with the decision support systems that need to be available to achieve success in the mission. It is the contention of this paper that the U.S. military needs a workable and understandable risk management system with the rigor to be comprehensive, the structure to be consistent, and the flexibility to adapt to a changing environment. The process must be able to identify and assess as many risks as possible across the enterprise of the service components and across the DoD infrastructure of the target GIG, and it must be a continuous process, which monitors the state of the GIG network and feeds back information to improve the process with every iteration. A comprehensive risk management system is designed to handle an eclectic mix of numerous network components and their interconnection and interfaces, and it is designed to handle large amounts of data required to make a trustworthy assessment of the systems risks so that decisions made to counter the threats are well informed and effective, contributing to the success of net-centric operations. The process is able to keep the management plan current with changing technologies, new threats, and up-dated military, political, economic and diplomatic strategies of the government. It is shown that this enterprise management system must take a top-down view as well as a bottom-up view, decomposing the risks across the myriad of networks, each of which requires special sets of values; then integrating the risk process across the many networks to establish a truly enterprise risk management system. This is especially important because DoD and the individual services have chosen to architect their networks in accordance with Service Oriented Architecture as discussed in Chapter II.

2. Beginning the Process Early in a Network System's Lifecycle

Viewing the networked system of systems from the top-level down, which comprise the infrastructure of the GIG, risk management of the network enterprise must be an overarching process, which includes and encompasses the risk management of the infrastructure's individual network systems. The challenge in a network of this size and

complexity is to mesh the overall risk management plan with the individual system's risk management plans, so that there is a unity of effort and a common set of objectives; and the most advantageous time in the system's lifecycle to start this is from the beginning during concept definition, which draws on the network system's concept of operations. If the risks to the network enterprise are not identified and assessed with the start of a management plan in place before the requirements and specifications are defined and allocated to system components, the architecting of the system during preliminary design does not consider how to architect the system to reduce or eliminate vulnerabilities that could be exploited, threatening critical data and system operation. In essence, the need for operational capability competes with the need for security; the resultant architecture being reactive to the threats as they are encountered during the later stages of the network's lifecycle.

E. PROPOSED NETWORK ENTERPRISE RISK MANAGEMENT PROCESS (NERMP)

1. Review of Available Software Risk Management Processes

The Computer Emergency Response Team (CERT) and the CERT Coordination Center of the Software Engineering Institute of Carnegie-Mellon University has been supporting network security for DoD for several years. Their model (Carelli & Young, 2008) for analyzing risk is a multi-dimensional model, which encompasses the following.

- Incident response risk model and assessment
- Software process risk model and assessment
- Operational security risk model and assessment
- Other risk models

CERT's classic model OCTAVE for operational security of computers and networks has the following steps.

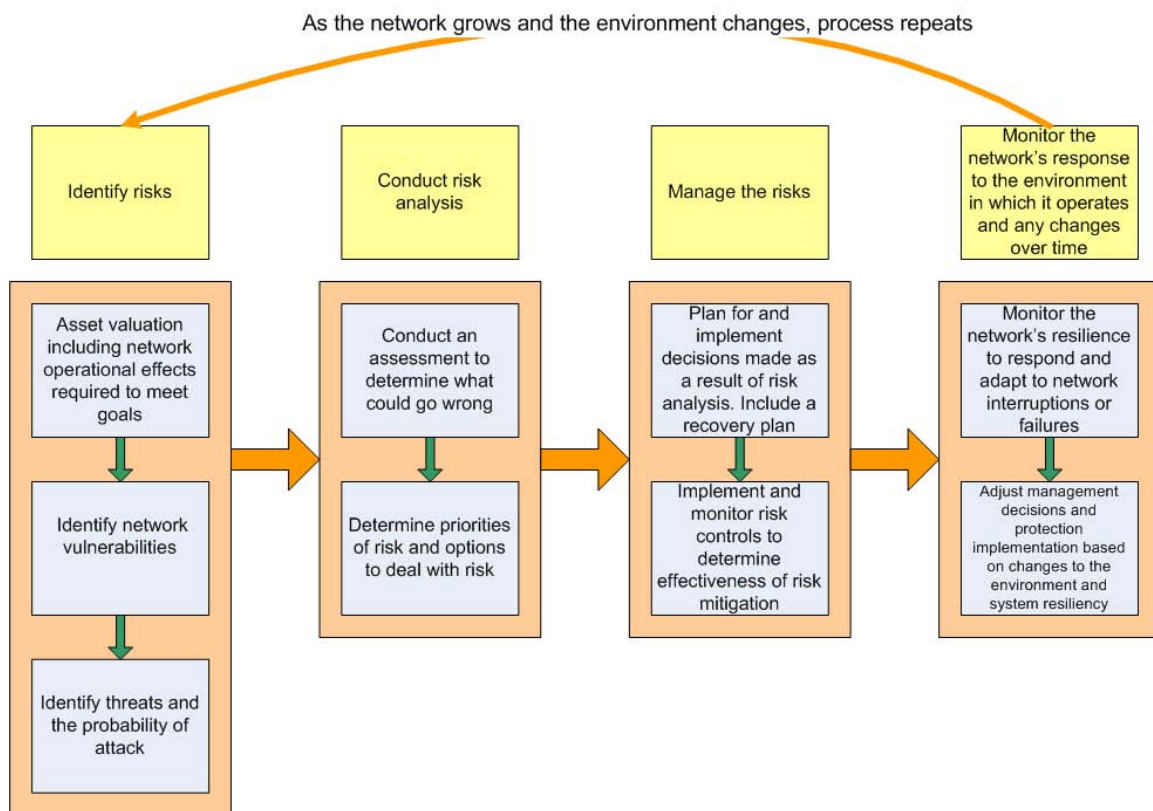
- Identify
- Analyze
- Plan
- Implement
- Monitor

- Control
- Repeat

This process is similar to the program risk management of the DoD acquisition program, and many of the activities of OCTAVE, surveys, workshops, questionnaires, and auditing mirror those of the program risk management requirements and activities of the DoD risk management guide for acquisition.

2. NERMP Details

Drawing on the process model from CERT, DoD Risk Management Guide for Acquisition, lectures and articles by Yacov Haimes, and course materials for enterprise risk management (Kujawski, 2009), Figure 14 graphically displays a process for risk management, which is discussed in detail below the graphic.



NERMP is similar to the process of the last chapter but is designed for network enterprises.

Figure 14. Network Enterprise Risk Management Process (NERMP)

The Risk Analysis Process is a method to identify the components of risk as stated above systematically and assess the risks identified to determine what could go wrong and assess the probability so that risks can be prioritized. The Risk Management Process continues the process once risks have been analyzed. It is then necessary to manage the risks by determining what can be done about matching available resources against risk implementation plans, and controlling and monitoring the network for the effectiveness of the risk management decisions as well as determining the effectiveness of survivability and resiliency measures for system recovery. Each of the components of risk, assets, threats, vulnerabilities (Figure 14, column 1), recovery and resiliency (Figure 14 column 4), are examined briefly in more detail below for their contribution to the risk analysis process as it applies to a network enterprise.

- Asset valuation is an important and complex part of the process. The value of network assets is more than just the cost of hardware, software and operational costs of the network. A thorough valuation must take into account the assets of information and functionality provided by the network and the value of these assets to achieving the organization's goals. This is a moving target, though. Information in the military is often transitory, valuable for the moment or the situation at hand. The effects that the organization is trying to achieve to meet goals is usually longer term, but even those change with changes in the environment surrounding the network enterprise. However, an honest valuation of assets in the identify phase supports the assessment of the impact of an attack on the network and where to place priority on the choices to handle and monitor the identified risks.
- Threat identification, assessment and management (such as it can be done) is equally as complex since the probability of an attack from a given threat agent is difficult to quantify statistically. Unlike reliability, a threat makes an attack based on the threat's subjective analysis of its likelihood of success in not being detected while doing the maximum amount of damage.
- Vulnerability of the network is the one risk component over which there is some control. However, in the age of COTS and SOA, identifying, let alone assessing and managing, the vast amount of ways to exploit a network enterprise as expansive and technologically complex as the GIG, can be overwhelming in itself. Several sources (Clark, Sollins, Wroclawski, & Faber, 2003; Chittister & Haimes, 2006; Haimes, 2009; Jones & Ashenden, 2005; McCabe, 2009; Storey, 1996) have approximated that in an individual computer operating system, there are

over 200 million lines of code, and out of those, two million have “bugs” (defects). The challenge is to determine what bugs are exploitable and what to do about them. Other vulnerabilities are explored in depth below.

- System recovery and resiliency are increasingly important to a comprehensive risk analysis. For the attacks that do get through, it is important to know how the network recovers, what information needs to be sustained during an attack and how quickly the network can get back to full capability after an attack. This analysis has to be conducted before an attack to make tradeoffs and decisions about what recoverability features need to be part of the network, such as redundancy, replication, diversity, and distribution. Survivability characteristics of recognize, resist and recover, are part of the requirements that comprise the other functionality performance parameters of a network.

The process, if done correctly, establishes priorities and allows for the selection of alternatives on which to make decisions on how and where to protect the system. Many of these decisions are made in uncertain circumstances, and the decisions made rely on some prediction of probabilities and of consequences. Since an effective risk management program must start in the first phase of a system’s/network’s lifecycle and continued throughout, an effective risk management plan guides decisions on how to architect a protected yet functional network that optimizes the competing objectives of system capability and system protection. As Yacov Haimes says of risk assessment and management, “The risk assessment and management process is aimed at answering specific questions in order to make better decisions under uncertain conditions” (Haimes, 2009, p. 22).

At the conclusion of the process, it should answer some of the following questions.

- What needs to be protected and why
- What is being protecting against
- How much protection is required
- How does the protection inhibit operation of the system and affect the desired outcome or ability to achieve the system’s objectives
- What protection is it possible to do without to make the system more functional
- What system functionality can be forfeited because of the unknown threat or vulnerability

- How is the protection to be implemented
- How much does the protection cost (to implement, in opportunity cost, in training and monitoring)

F. IDENTIFYING, EVALUATING AND MEASURING THE ELEMENTS OF RISK ANALYSIS AND ASSESSMENT

1. Asset Valuation

Appraisal of an asset is important in that its value depends on the end product or mission that asset is designed to achieve. For instance, given a similar information system

Asset valuation including network operational effects required to meet goals

in two organizations with similar vulnerabilities in that system, an adversary who successfully exploits that vulnerability causes greater damage to the organization with the more critical mission. As with any system design, development or operation, the engineer needs to know the systems requirements, how those requirements are going to be or are being met by the system architecture, and if the functionality of the system is designed to achieve the objectives of all the stakeholders. An assessment of risk must also start from the vantage point of a thorough knowledge of the system under assessment. A detailed system definition comprising the system's requirements, specifications, and objectives is required before an assessment of the system's vulnerability's is determined. In several studies on risk assessment of networked computer systems, and especially in Storey's analysis of safety-critical computer systems, the first step in the study of system risk is to discover asset value (Jones & Ashenden, 2005).

Placing value on network assets is not just about the dollar value of the information asset exploited, but also about the consequences that exploitation has on the organization in terms of missed opportunity or damage to critical data, people or infrastructure. Not only is the consequence of any given exploitation important, but so is the interrelationship of the value of that system to the value of a connected system and the cascading effects that an intrusion and attack on one system may have on another. In the DoD enterprise, this process is problematic because of the large inventory and wide diversity of networked information systems now used for a host of capabilities


throughout the services. Add onto this, the direction of the new architectural framework in the form of service oriented architecture, and the effect that one system's degraded condition can have on the condition and capability of another is endless. There are so many systems and so many people and organizations at stake with opinions as to whose system is more important. Additionally, a networked system takes on different values depending on the operation for which it is used, the environment in which it is operated, and as envisioned by FORCENet and the GIG in general, to be able to set up ad hoc networks, and what the value is of a network as the composition of that network changes to achieve a temporal objective. The military has employed a similar system of information valuation since the beginnings of safeguarding classified information; that level of classification has been determined by the severity of its loss to the conduct of U.S. operations. For instance, the loss of top secret information would cause grave consequences to U.S. operations and to U.S. forces should it fall into unauthorized hands. This same idea, but on a far larger and more rigorous and robust level, is needed to place a value on the multitude of networked systems in the service today and planned for the future in the GIG. The Navy has taken the initial steps in this type of classification by the development of Cross Domain Solutions and Multi-level Security (CDS/MLS) processes within U.S. information systems. However, with the fluid nature of these systems' capabilities as they relate to the environment and the national security situation, and as they transform with the addition of changing technologies, it is necessary to conduct a top-down analysis of system value both as a stand-alone system and in the context of interoperability (and with SOA) and collaboration with other systems. With the desired capability of creating ad hoc networked systems to meet a tailored mission, the valuation of individual systems changes and must be addressed each time one of these ad hoc networks is created.

Taking a mission-oriented perspective, Donald Buckshaw et al.(Date?), take a back door approach to asset valuation by modeling a value hierarchy on the adversary, the user, and the service provider. Instead of trying to optimize the system under a model of multiple competing objectives, they use Value-Focused Thinking methodology introduced by Keeney and Raiffa. Their main focus on assigning value was to an

adversary model, but they also applied this methodology to a valuation of assets in their user and service provider models to help quantify the importance of assets from a mission-oriented perspective, which then leads to an assessment as to the severity of the consequences due to an attack on a networked system. Appendix B examines this model.

2. Vulnerability Determinations

Hand in hand with the threat assessment piece of risk assessment is a determination of a system's vulnerability. Without a vulnerability element, the threat



Identify network
vulnerabilities

agent cannot harm the system, and without a threat, the vulnerable part of the system is not a risk (other than normal reliability considerations). The interrelationship of threat to vulnerability is captured in the attack tree analysis mentioned in the next section. The path an attacker might take to reach an

objective of doing harm to the system leads into an analysis of the scenario that points to the vulnerable elements of the system and what components of hardware or routines in the software might be vulnerable and require attention. This is done routinely in the commercial world with the identification of a path or scenario an attacker might take and identification of what components are exploitable. For instance, in 2007, it was found that no matter how carefully a network topology is guarded within the network, it is possible for an intruder to gain network knowledge while packets are transiting the Internet through a process called reverse Domain Name Server (DNS) look-up. Transmission Control Protocol (TCP) packets were captured on the Internet, which gave internal IP address information to an unauthorized source (Faber, 2009). There are ways to prevent this with the configuration of the network's DNS servers to keep reverse look-ups internal to the network, but this vulnerability is illustrative of the breadth of system vulnerabilities and the huge task at finding and fixing them.

Determining the vulnerability of a system is a very complex problem. In networked information systems, vulnerabilities can be extant in system software (most visibility these days), hardware, firmware, user or service provider personnel, policies and procedures, or in the common practices of use and applicability. In the software

sector alone, vast libraries have been compiled to document and catalogue the myriad of vulnerable components, programs and paths in the vast array of computer systems and networks. Vulnerability can show up at any level of the system from the physical layer to the most advanced application. In addition, because of the complexity and diversity of the technology, the path to a vulnerable component can take many different routes depending on the instrument or method used to penetrate a system.

Vulnerabilities are a natural byproduct of the quantity of systems which have been developed with quality that is less than perfect, incomplete requirements, and limited testing. The higher the quality, the fewer vulnerable components, but it is now more difficult to detect the remaining software flaws. Quality of software was discussed in Chapter II, with the discussion of CMMI; a process for quality control on software development, which is a process to improve the level of software quality to diminish the suspected software faults that open up vulnerabilities in the software architecture. Software and systems engineering need to grow in scope and capability because even as the quality of software products improves, other additions to the software inventory open up new paths to exploit an upgraded system, making it difficult to catch up. On the software side, patches have been used in commercial and military enterprises to fix or lessen vulnerability when it is discovered. It is by far easier to find and fix vulnerability during the development stage of a system's life cycle than when the system has already been deployed. However, the use of COTS components and programs makes this problematic. In fact, one of the down sides to open architectural development and reuse in a SOA is that the developer may have little if any insight into the contents of a software program or a component with imbedded software and its vulnerabilities. This is especially true of purchased material (programs and components) design architectures, which are proprietary. Some of this risk can be mitigated by disabling portions of COTS programs not being used, layering additional security programs on top of the proprietary program (but this may itself create more vulnerabilities), conduct research and development into technological tools to analyze the COTS coding (this is an expensive alternative that must be weighed in the risk assessment), or plan on a response mechanism or procedure for fixing flaws (more expensive but probably necessary is the

capability of fixing flaws “on the fly” to improve recoverability) (Anderson & Hundley, 1998). COTS use in building systems has gained wide acceptance within the military’s acquisition community because it saves on system development costs, on personnel training costs (many users have used like systems in the commercial world), and on the costs of inventory stocking and supply chain management (although some control is lost when relying upon a vendor for spares, and when dealing with multiple vendors, the problem can multiply rapidly). While the cost advantages of using an open architecture approach to design of networked systems looks appealing, the remedies cited above can come with their own enormous price. Neil Storey (1996) notes in his book, *Safety-Critical Computer Systems*, that exhaustively testing a piece of software can be time consuming and costly to find all the vulnerabilities (what he calls exhaustive testing) in just one piece of a program. The procedure must test for all possible binary inputs to a system against their output (black box testing when the code is unknown as in proprietary software) .He points out that” With a small program of 40 inputs, the test involves the input and measurement of output of 10^{12} combinations. When the subsystem components are known, a check of each component as its state changes (binary patterns) can be conducted, but in a simple 8 byte microprocessor, exhaustive tests of all combinations of states will be $10^{160,000}$, and to only look at the combination of failures due to a bridging fault on just three nodes, would require 10^{18} combinations.”

Obviously, to test a component of COTS software for vulnerabilities, sampling techniques must be used (what Storey calls coverage-based testing) to develop statistical measurements, which gains a confidence level that a system’s vulnerabilities are limited. Still, many vulnerabilities may and probably do exist.

One of the difficulties in looking for vulnerability when conducting the risk assessment process is that as technology improves at a rapid pace, the risk management methodologies are slow to react to incorporate the new technology and to identify the new vulnerabilities created by the new technology. The challenge is to maintain a vulnerability that is accessible and current with the range of vulnerabilities to the system’s network, the various operating systems on that network, and the ever expanding quantity of applications in each information system, and the connectivity protocols used

for interoperability. The vulnerability library provides the latest known or experienced paths that lead through the system's vulnerabilities and the ways to block these paths. In addition, the vulnerability library needs to remain current with the technology of vulnerability detection devices and intrusion alert mechanisms. All of these factors are important to the analysis of the risks the network faces and to the assessment with which they are dealt.

When considering the system's vulnerability, the security specialist must look at detecting intrusions into the system's vulnerabilities, identifying the vulnerability to be exploited, and the proper countermeasure to prevent the intrusion from proceeding. In addition, consideration must be made as to how the system maintains its minimum or critical functionality if the intrusion is successful, and how the system limits the extent of the intrusion and stops any progressive or cascading effects to the system due to the intrusion. Many methods exist for intrusion and vulnerability detection including Rule-based pattern recognition, forced intrusions to make the system react before an attacker penetrates the system, and inference-based testing to recognize the interrelationships between components in the threat environment. Identification of the intrusion once detected is important to know how to stop it. Access to a database that catalogues known malicious agents is important to identification and resolution of an intrusion on a system. It is also a key element in the identification of countermeasures, which can be applied in the planning and design of a system or during operation and recovery of the system once an intrusion has been detected.

Taking the analysis of the threat agent and the system vulnerability that the threat agent might exploit is one of the key elements in the calculation and assessment of risk, and is crucial in managing that risk.

3. Threat Assessment

A threat to a distributed networked information system is comprised of an adversary (an entity with intent to cause harm or disruption) who uses tools (viruses, worms, information overload, software altering devices) to produce an undesirable effect (information denial, corruption, theft, fabrication), which reduces capabilities or causes

harm in safety-critical applications. The military make its business out of knowing who the threat is today, but it is quite uncertain who the adversary is going to be in the future. Also, in today's environment with an asymmetric enemy, it is the opinion of this paper that the identification of the threat can get muddled in the identification of the loyalties of the threat and ideals that motivate them. By not knowing whom the adversaries are, one is less certain of the tools they might use, what their motivation is, and what effect they want to inflict on the distributed network system.

Much work has been done both in the public sector by the major producers of software and computer and network systems, and in a less visible manner, in the military

Identify threats and
the probability of
attack

to categorize and recognize the vast array of methods and tools available to an adversary. The major effort has been in building libraries of threat data and techniques with appropriate remedies. In the simplest terms, companies such as Symantec and McAfee who sell remedies to private consumers through distributed software and routine programs maintain the libraries in the public sector.

To be classified as a threat, a threat agent needs to have opportunity, motivation, resources, inside knowledge, and a finite amount of time to accomplish an objective. If it is too hard to penetrate a system, or once penetrated, too difficult to achieve the desired effect (such as denial of service), or it takes too many resources or time, or the desired effect does not have the impact that would make it worth the expenditure of those resources, then the likelihood of the adversary actually attempting to breach a system becomes less. It is also possible that other inhibiting or amplifying factors may come into play to make an entity a threat. Deception can act as an inhibitor and perceived lack of retribution can be an amplifier.

The assessment of the threats that are a potential risk to a networked system is an integral part of the overall risk assessment and management of those risks. Most methodology for determining the source and the qualities of a threat (Jones & Ashenden, 2005; Buckshaw Parnell, Unkenholz, Parks, Wallner, & Saydjari 2008; Hamdi & Boudriga, 2005) rely on finding a logical grouping of agents to decompose further into

their motivation, capabilities, and resources as well as the triggering factors, or catalysts, and the timing that would cause a threat agent to exploit a system's vulnerability. Each of these categories can be further decomposed and weighted on a constructed scale (when no natural scale is available). In their Mission Oriented Risk and Design Analysis (MORDA) model of risk assessment, Donald Buckshaw et al. (2008, p. 24) use what they call swing weight matrix in their determination of value for the level of threat to a system as well as the other components they consider in their assessment of risk. The swing weight matrix consider the change in relative importance between different measurements of value when the value measurements go from worst to best possible level. An overview of their methodology is contained in Appendix B, examples of risk models. It is important in any assessment system to weight the factors properly relative to one another, to know why the weighting is being distributed a certain way over an alternative. Since much of the input data used in a given methodology is subjective in nature, it is important to process that data in a logical sequence so that the process is repeatable (especially if the model is used in a continuous analysis) and the results obtained are consistent and justifiable within the constructive scale chosen. Finally, the results have to be useful for decision making, which requires an understanding by the decision maker of the basis on which the decision is being made.

When looking at threat amplifiers (events or motivating factors that encourage attack) and inhibitors (change in cultural attitudes or political roadblocks) in regard to a specific threat agent, the effect the amplifier or inhibitor has on the agent must be considered, on the environment in which the agent and the protected system exist and on the system being protected. Consider an amplifier of a search for recognition by a threat. It has an effect on the threat and the system, but the environment may not come into play; whereas, the speed in which technology changes and improves affects the system and the environment, but any adjustment to the magnitude of change probably does not affect the threat agent.

As one piece of the puzzle of gaining an understanding of the risks to distributed networked systems, a knowledgeable threat assessment provides an overall risk assessment with valuable information. Without a threat, the fact that vulnerabilities exist

in the information systems becomes academic; an exercise in technological expertise to plug the holes and reach a certain level of perfection. However, this is certainly not the case. Numerous threats are present and are waiting for the right time to exploit networks to achieve the goal of degrading or incapacitating information capability. The threat is not just from the outside (although outsiders may already have achieved a position inside U.S. systems, either with “time bombs” in the software or by compromising users). The Computer Emergency Response Team (CERT) at the Software Engineering Institute has examined case studies of insider malicious activity to include sabotage, espionage, fraud, theft, and manipulation. They have developed a simulation to help uncover potential cases of insider malicious activity through the use of behavior modeling and the consequences of improper applications of new technology as well as practices for personnel screening and authorization to systems. This study has focused lately on the potential for insider activity during the system’s development lifecycle, where virulent code has been inserted during development among other deleterious actions that may take years to uncover (CERT, 2008). Knowing the threats and planning for their reduction is an important step in any risk management process both before a system degrades or fails and equally important when planning the operation of a system at reduced capability and how to recover as quickly as possible.

4. System Recovery

A subsequent chapter explores what makes a system survive in a hostile environment, particularly a distributed network of information systems relying on one

Monitor the network’s resilience to respond and adapt to network interruptions or failures

another for complete functionality and the ability to meet objectives, and how network survivability is inherent in the network enterprise risk management approach. This section examines an overview of what element recoverability plays in a risk assessment process and what is meant by reactive risk analysis. Most methodologies and risk assessment models focus on a risk management scheme to prevent the undesirable outcome. This is why recovery or reaction is routinely left as an afterthought in most risk assessment models. Once a threat has exploited a system’s vulnerability and achieved its objective (disruption, theft, or denial of service),

the risk has manifested itself. Therefore, what does reactive risk and system recovery have to do with risk assessment, and why should it not be subordinated but treated as an equal step in the risk assessment process? Principally because it cannot be avoided or all risks mitigated to zero, and with a system as complex, and with such determined and ingenious adversaries, it is not a question of if but of when; and it is absolutely necessary to be ready for this eventuality.

The major measurement of reactive risk assessment is time and the major tool in the risk assessment arsenal to handle this ability to react is the intrusion detection device. The element of uncertainty in this case, which makes this applicable to the risk management process, is how much time is available for a given attack, how much time before losing the minimum amount of capability needed to accomplish the mission, and does the intrusion detection give the system time to react, or more simply, does it detect it at all or does it detect too much (false alarm). In the survivability chapter, quantification of these survivability characteristics are examined by exploring some system models using optimization and simulation to characterize the survivability of a network. The critical element in these models is what value these characteristics provide the survivability of the network for it to meet requirements. The other critical element cursively mentioned in the model is how the requirements for survivability are determined and at what point in the system life cycle should the survivability requirements be decided. The contention of this thesis is that protection, risk mitigation and survivability system/network requirements must be integrated into the general requirements definition phase, and they ought not to be dealt with apart from the rest of the systems engineering process.

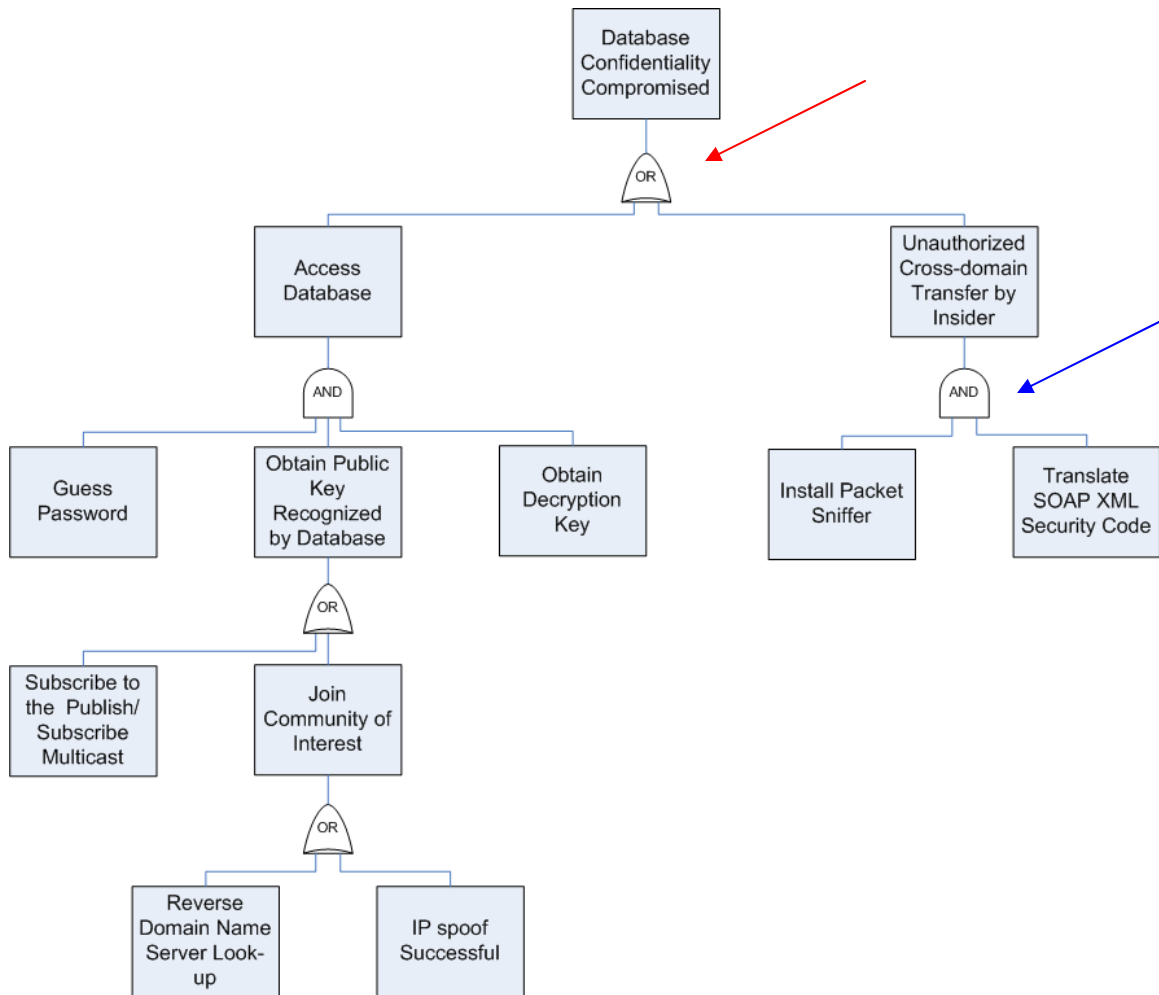
G. ATTACK TREES: A USEFUL TOOL IN RISK IDENTIFICATION AND ASSESSMENT

Drawing at once on the concepts of game theory and fault trees used in reliability analysis, attack trees can be useful in identifying and analyzing network vulnerabilities and the paths that can be exploited to gain access to the assets of the network. At the same time, they are useful in gaming the attributes of a threat that would make the threat more or less likely to make an attack on the network. As discussed above under threat

assessment, a threat agent has multiple motivations on whether to execute an attack or not to attack a network with multiple constraints. Several of the risk management process models discussed in Appendix B use attack trees in their identification and assessment of network vulnerabilities and the motivating factors of threat agents (Buckshaw et al., 2005; Hamdi, 2005; Hernandez, 2001; Jones, 2005).

1. Identifying and Correcting Vulnerabilities

Attack trees use the same methodology as fault trees in analyzing the paths to system faults when determining overall system reliability. The attack tree, shown in Figure 15, takes the ultimate objective of the attacker as the root of the tree, then expands the tree through the different logical steps an attacker would be required to take to reach the ultimate objective. Developing the attack tree leads network developers to discover where the networks vulnerabilities are and the paths to get to a vulnerable network attribute. Analysis of the attack tree paths also reveals methods to eliminate or reduce the vulnerabilities, while in turn informing them of what the effect on system functionality might for certain remedies to fix a vulnerability.



Attack tree analysis of the route an attacker takes helps to organize the evaluation of network vulnerabilities and identify those needing to be fixed.

Figure 15. Sample Attack Tree Analysis of a Threat

In Figure 15, the logic operators, AND & OR gates, identify either alternative paths to the ultimate objective (OR) or the combination of steps required to reach the next level (AND). For instance, the OR gate (red arrow in Figure 15) affects database confidentiality since it is vulnerable from either access to the database proper or from an unauthorized download of information to a network enclave of lesser classification and easier access directly from the Internet. The AND gate (blue arrow in Figure 15) acts on

the unauthorized cross-domain transfer by requiring the use of a packet sniffer and translation of XML security addressing to get to the information unintentionally moved to a less secure location on the network.

2. Minimal Cut Sets

Minimal cut sets (Haimes, 2009) in the attack tree can point the analyst to the likely scenario of attack and where to look within the individual components of the system for the vulnerabilities requiring the most attention. The minimal cut set is the minimum set of attack nodes an attacker needs to take to reach the top goal of the attack. Additionally, the analysis of possible scenarios following certain paths through the attack tree can lead an analyst to discover patterns in the way attackers reach their objectives and may be supportive in developing strategies to counter similar scenarios in multiple network systems. Attack patterns can be built into scenarios, which take into account the following.

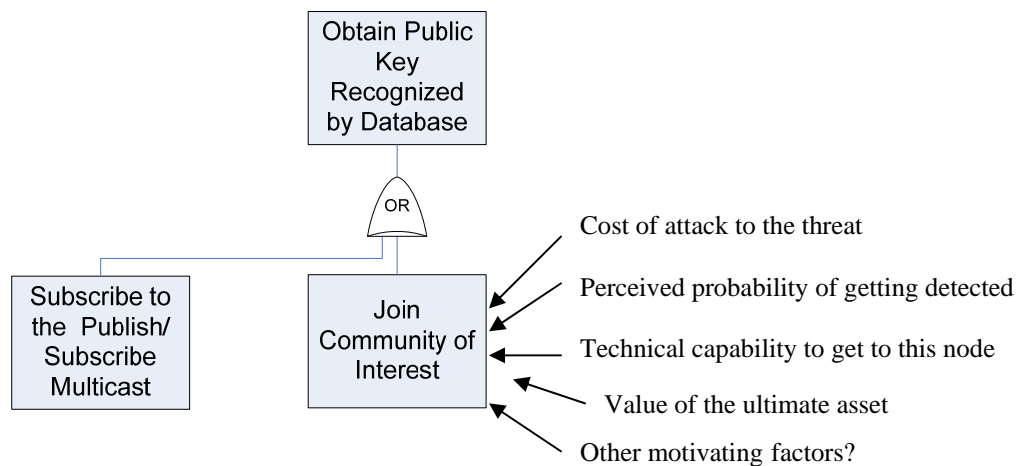
- Attack objective (base data)
- Preconditions set to motivate the attacker to achieve the objective
- Attack mechanisms, tools, paths chosen, etc.
- Changes to system state as an attacker proceeds down the scenario path to achieve the objective

This analysis leads into the second part of the game theory of the attack tree analysis; identifying and analyzing the threat attributes leading an attacker to choose a certain vulnerability path. This analysis supports the decision of where to allocate resources to mitigate the risk from a given vulnerability.

3. Identifying and Analyzing Threat Motivations and Constraints

Similar to the quantitative analysis of the fault tree, the probability of a threat choosing a primary entry point on the attack tree coupled with the likelihood of being able to proceed to the next step yields a value of risk with each step. For a given path up the tree to the ultimate objective, the probability that a threat would reach the ultimate objective is calculated similar to the composite failure rate calculated from a fault tree. However, as shown in Figure 16, the quantitative values at each node of the fault tree

consist of a n-tuplet of subjective values, the cost to the attacker, the level of technical capability of the attacker to reach that step, the attacker's perception of the likelihood of being detected before or during an attack, the attacker's perception of the value of reaching the ultimate goal, and other motivating factors. If a reasonable quantification of the values associated with the attacker's several motivating factors can be agreed upon, and a reasonable limitation to the number of values can be reached, it might be possible to achieve a quantitative value for the probability of each attack path for comparison and determination of where countermeasure resources should be allocated. This calculated value is called the propensity for the attack path by Amenaza Technologies (Ingoldsby, 2009).



Attack trees can be used in a game theory approach to evaluate an attacker's motivation. Enumeration allows comparison of the different paths to determine the most likely route an attacker might take to get to the objective.

Figure 16. The Attack Tree from the Attacker's Perspective

Carrying this methodology a step further, a network of arcs (paths) to get to successive nodes (components in the system and similar to the nodes on the attack tree) can be formulated and analyzed using various network analysis tools to determine the shortest path to reach an objective and changes in node states that would indicate the presence of an intruder (Hamdi & Boudriga, 2005). In attack tree analysis, the preconditions, post conditions, and the steps are combined into each node on the attack tree. In network methodology, conditions are separated from the steps between arcs and

nodes. Both analyses give more rigor to the threat assessment of the risk analysis process and lend themselves to the development of better intrusion detection devices, and other network vulnerability containment features. It also allows the analyst to consider scenarios involving multiple attackers on one system that may desire to conduct a coordinated attack. Computer models have been developed that consider the coordinated attack as the union of more than one individual attack scenario and seek to model the system's states as a coordinated attack occurs.

H. SUMMARY

Network enterprise risk analysis is an important part of an IA program and it should be implemented at the beginning of a network system's lifecycle. The risk analysis and management process follows the steps of general risk management processes for safety, program, operational, and enterprise risks in organizations. Unique to network risk management is the concentration on an unpredictable threat who is motivated to exploit network vulnerabilities that the threat discovers for an ultimate goal of gaining something of value.

The network risk management process identifies, assesses and manages risks to the network by implementing mitigation strategies to reduce vulnerabilities and improve network resiliency through recovery and survivability techniques. With mitigation strategies in place, the process then requires that the network be monitored for the results of the mitigating actions to observe effects on network functionality and the network's ability to resist or handle threats. Based on the effectiveness of the mitigating actions as observed by monitoring or by changes to network requirements or the environment surrounding the network, the risk management process is taken through another iteration to support improvements to the networks adaptability based on experience.

Attack trees are a useful tool in analyzing network vulnerabilities and assessing the motivating factors of threats to attack a network.

V. NETWORK SURVIVABILITY AND RESILIENCY

A. INTRODUCTION

This chapter examines what survivability and resiliency mean and why the concept is important as part of a robust network enterprise risk management process. It explores some of the ways to make a network more survivable and resilient. It also discusses the basic framework of select system models developed by academicians for quantifying network survivability, what the quantification of survivability can do to support improving the risk management process, and the limitations of the models in providing concrete evidence for quality decision making in global networked system of systems built on the scale of the GIG and systems based on Service Oriented Architecture.

While risk analysis and management are designed to find and fix vulnerabilities that put the network at risk by the threat that exploits them with the intent to gain access to valuable information system assets, survivability is the attribute of a system that defines how it deals with an actual exploitation of network vulnerabilities that have remained after mitigation implementation. The architecting of a system before attack to respond to attack after other risk mitigation implemented plans have been activated to resist attack by mitigation plans has reduced network vulnerability. In other words, survivability and resiliency are defense in depth for a network by designing the capability to continue action to resist and recover after an attack scenario, not just the mitigation strategies put in place before attack. While it is vitally important to manage the risk to a network before attack and to make every effort to keep it from happening, a further defense mechanism and process needs to be in place in the event of an attack.

For many of the critical networks upon which military forces rely to obtain the information needed, it is essential that their critical networked communications and applications be designed to survive, because by nature, they are exposed to a hostile environment. It is highly probable that an adversary is attempting to disrupt the military's computer networks and their networked operations to gain the edge in any level of

operation, from high intensity conflict to stabilization and peace-keeping operations. If a network can be designed or modified to be more survivable, it can strengthen its defenses against those risks for which it was unable to mitigate or remove fully prior to attack. This adds flexibility to the management of risk up front, allowing for greater options when deciding how to deal with the risks identified at the beginning of the risk management process. This is especially important when managing the risk on critical network systems since any intrusion, no matter how small the probability, could put important operations in severe jeopardy. Not only is it desirable to architect a network less vulnerable to failure (failure being deliberate or accidental intrusion or because of hardware/software malfunction), but also design the network to be resilient and adaptable under attack and failure, and to be able to recover in time to minimize the disruption to the completion of critical tasks. The ultimate goal in architecting a network for survivability and resiliency is to improve its operational effectiveness, safety, and affordability through the refinement of technical effectiveness, system effectiveness, system availability, and cost controls (Ellison Fisher, Linger, Lipson, Longstaff, & Mead, 1999).

B. DEFINING SURVIVABILITY AND RESILIENCE

1. Network Survivability Characteristics

a. Susceptibility

Susceptibility is the capability (or lack thereof) to avoid an attack. It is essentially the converse of looking at the threat agent. Chapter IV discussed using a game theory approach with the attack tree method for analyzing a threat's motivation and capability to exploit a vulnerability and conversely determining which paths through the tree are most vulnerable so the vulnerability can be mitigated. Susceptibility approaches the game theory from the standpoint of analyzing for the network's strengths and tactics; particularly the network's ability to recognize an attack and avoid it. In any system, susceptibility can be reduced by using decoys/deception, removing the system from the adversary's theater (or not letting network boundaries interact with the adversary's system boundary), and by the capability to recognize an attack on the system (intrusion

detection) in time to take evasive or defensive action. In a computer network, this can be accomplished by the correct design and operation of intrusion detection devices, policies as to when and where networks are accessed, and tactics as innocuous as the “honey pot;” drawing an adversary to a place on the network that looks appealing, but is a trap to keep the threat from reaching valuable data, applications or network functionality (Ellison & Moore, 2001).

b. Vulnerability

In survivability and resiliency analysis, susceptibility is vulnerability go hand in hand. When looking at a network’s vulnerability from the survivability perspective, the system weaknesses and the paths adversary might take to exploit the system to achieve an objective are not the only factor. Also, an analysis of the interrelationships between known areas of exploitation for the effects of that exploitation must be done; what the immediate damage to the system would be and if the effects cause a progression of damage to the network in a linear or cascading (arithmetic, multiplicative, or exponential) manner. Survivability analysis seeks to define where damage could occur on the network, what the extent of the damage is and how that changes over time, and what methods or technology might be employed to limit or stop damage to the network once an adversary has discovered and begun to exploit that vulnerability (Ellison & Moore, 2001).

c. Recoverability

Analysis and design for recoverability of the networked system parallels reactive risk management processes and methods described in Appendix C. Recoverability is the quality of robustness displayed by a system that can return to normal operation after an attack by a threat agent. Recoverability is the robustness of a system to return to normal operation after an attack by a threat agent. It is defined by how the system and the operators respond to an attack. However, the recoverability of a network must be designed into the system both technologically and procedurally. In critical networked computer systems, continued operation in the face of an attack may require instant response and can only be controlled by an automatic response mechanism

such as a switchover or an auctioneered system that can assume the critical capability. If time is critical but not immediate, system design should consider the intermediate stages that can be recovered in the face of an attack and still maintain critical functionality. Also, consideration must be given to the network's capability to provide critical services at a reduced capability for an extended period of time and how much and how long degradation to the operational objective is permissible until full system recovery or until the objective is not attainable even with later recovery. An important aspect of recoverability is the ability of a network to adapt in the face of an attack and to learn from that adaptation to make the network more resistant to future attacks. However, as the system becomes more resilient to attacks through experience, the threat agent can, and does change tactics. The ultimate capability of a recoverable, adaptable system is to learn from the present attack and be able to predict how the next attack morphs so that the system is less susceptible to the next attack. How to design perspicacity into a global networked information system can be somewhat problematic (Ellison & Moore, 2001). In networked system, it is important to design in redundancy and dispersion/distribution (through enclaves or other separation schemes). When the attack has started, the system must be able to redirect the energy of the attack (denial of service redirected to an inactive server), systems designed for optimum fault isolation and load shedding, ability to compensate for services or capabilities that are damaged or stolen, and the adaptability to recombine system components automatically to reconstitute critical services. On top of the automatic adaptations, procedures and operator instructions that are pre-planned and practiced to reconfigure network connections and even architecture are necessary for continued uninterrupted operation and continuation of critical operations

2. Designing a Network for Survivability

a. Designing Survivable Networks at the System Boundaries

Designing a network for survivability is scenario-driven by the scenario of an attack by a given threat to the network. The architectural decisions are dependent on what the attack might be and the probability of the attack. However, the architecture is also guided by the requirements definitions. The challenge in designing survivable

systems is to determine how to define the requirements of a survivable and resilient system since survivability depends on the type, timing, and depth of attack. During the requirements definition phase of a system's lifecycle, requirements are defined and given specifications based on the Concept of Operations (CONOPS), which is used to determine the system's capabilities. The CONOPS is also scenario driven, but with the scenario desired to meet the organization's goals derived by effects-based thinking (the effects the organization desires to achieve from the operation of the system, among other actions). However, the CONOPS scenario is somewhat deterministic whereas the threat scenarios are stochastic.

One location in a network (or any system for that matter) where the probability of attacks from threats can be somewhat constrained is at the system boundaries. Much the same as in movement warfare, designing a network for survivability and resiliency depends on where the line is held against attack, or what system boundary is the last strong-hold to ensure the network delivers required critical services in the face of attack. As seen in the attack tree analysis, the attacker enters into the network by exercising sequences of interdependent decisions to produce (the attacker hopes) undetected and disastrous consequences to the functionality and information of the network. McCabe Software[®] uses a software validation approach to check for trustworthiness of software paths and to uncover security flaws in software code by analyzing the control flow paths and verifying control flow integrity. This method is a way of drawing the line (at the network boundary as defined in the requirements) on an adversary's attack (McCabe, 2009).

b. Designing Survivable Systems with COTS Software

Designing networks for survivability and resiliency with COTS software as prescribed by open architecture requirements can be problematic because of the lack of access to the COTS software artifacts or the COTS engineering process when COTS are used in network system development. Controlling system states is important throughout the development cycle of software development, and access to the artifact and engineering process of COTS is important in providing the assurance evidence for the

trustworthiness of the developed software. As the realization that software is becoming the overall cross-functional systems integration agent, one way to provide this assurance is through the methodology of the Capability Maturity Model Integration (CMMI) levels of software development (Chittister & Haimes, 2006). Another way is through the methodology of a Vendor Risk Assessment and Threat Evaluation Project[®] offered by the Carnegie-Mellon Software Engineering Institute CERT. This methodology examines the COTS product used in software development from the vendor's inherent risk elements (visibility of artifact attributes, vendor performance history, trustworthiness, vendor technical competence and compliance to standards) and the vendor's risk associated with the developer's risk management skills in dealing with vendors (technical and non-technical risk mitigating factors, exposure, vendor compatibility, independence and interdependencies) (Ellison, Linger, Lipson, Mead, & Moore, 2009). The human knowledge role in software development should not be overlooked when designing for resiliency.

The focal point of systems integration is the realization that all hardware-software systems are made of multiple interdependent sub-systems. Each sub-system, in turn, is a system that is driven by its own state variables, inputs, outputs, and control and random variables, among others, where the output of one system constitutes the input to others. Understanding this interconnectedness and the interdependencies among these many sub-systems is imperative for an effective software architectural design and for ultimate systems integration and control. (Chittister & Haimes, 2006, p. 9)

c. An Example of Survivability and Resiliency Scenario-Driven Requirements

If survivability and resiliency requirements can be defined at the network's boundaries, and an analysis of the important (most probable or most devastating) threat scenarios can be analyzed for flow control paths using attack tree analysis, then this data can be used in a survivability/resiliency analysis to study the effectiveness of the network Intrusion Detection Systems (IDS), and reaction/recovery mechanisms to meet minimum standards for connectivity, time and amount of lost data (as in packet loss in an IP network), and mechanisms and software processes to establish and safeguard data in priority order. The survivability/resiliency studies support the

determination of which survivability primitives of redundancy, replication, distribution, separation, access control, diversity, or adaptive reconfiguration contribute most to making a survivable, resilient network. Consider the following example of possible survivability requirements driven by the following threat scenario.

It is desired to interconnect in an information systems network a sensor system, an intelligence analysis system and a weapons control system to detect, track and engage a theater ballistic missile attack. To accomplish the objective, the weapons control system must receive information from the sensor network, validation of the target from the intelligence analysis network, and verification of weapons parameters from the weapons control network to engage and destroy the target. Risk analysis determines that the highest probability threat and the weakest vulnerability to the networked system of systems is the alteration of missile identification parameters in the intelligence network. Without valid missile identification, the weapons control system does not allow engagement of the target missile. From the attack tree analysis, a path of a threat agent leading to missile identification data is mapped. Survivability analysis looks at the probability that the intrusion can be detected as the threat nears the goal of altering the intelligence network, how the damage to the system progresses over time, what level of damage can be tolerated before the correct information has to reach to the weapons control network to achieve successful target engagement. Resiliency analysis examines how quickly the intelligence network can stop the intrusion, determine what data was corrupted, what data is trustworthy, and how soon the network can return to normal or how quickly it can switch to an alternate network path unaffected by the intrusion.

While the quantification (such as it is) of the impact of a network compromise during the survivability/resiliency analysis is similar to the impact variable in preventative risk analysis, the probability has shifted to the network's ability to recognize, react, recover and adapt as opposed to the probability that the intrusion happens in the first place. As part of the design of the survivable system, the goal is to determine the probabilities attached to recognition, reaction, and recovery for a given intrusion and to build a system that recovers or adapts in enough time to meet the system's mission. When the important threat agents are considered, their interactions at the boundaries of the network have been studied, and the possible ways they could penetrate the network and cause damage from attack tree analysis using a type of game theory, the aggregation, even from a holistic perspective, of the scenarios that a threat

might come from is no small matter. Moreover, with the changing dynamic of a network's objectives (especially an ad hoc network in a wireless or satellite communications mode), designing resiliency into the network to secure its assets and functionality requires the design to be adaptable to accommodate the changing objectives.

d. Challenges in Quantifying Survivable Network and Software Attributes

Quantifying survivable network attributes requires the determination of what attributes of a network make it more survivable and how they are quantified; attributes such as connectivity ratio, quantity and quality of information transmitted and received, service request distortion percentage, maximum service disruption time, and node (server) state. To improve the survivability of a network, design trade-offs need to be considered between network functionality under normal conditions and system requirements to meet mission objectives under selected attack scenarios and which of the network's attributes cited above are most important. Survivability analysis of computer networks and the network software controlling operations has peculiarities that differ from survivability analysis of traditional hardware systems. Software, the largest component of networks and arguably the most vulnerable, can be attacked by almost anyone with some knowledge of computer systems and programming to varying degrees. It is not susceptible to obsolescence, and it is particularly difficult to uncover all its faults (especially in COTS as noted above) and to intrusions that might introduce additional faults. The faults are not randomly distributed between a class of software as with component reliability and survivability of hardware components of the same type or makeup, so software faults can defy accurate prediction. While some of the same tenets of design primitives, which make a physical system more survivable, hold true for software systems and computer networks such as geographical separation, redundancy of units, deception techniques, and human access control; software and network systems offer unique characteristics, which make some design primitives indispensable when dealing with information generation and information flow. Duplication and rapid replication of data and recovery of connections in networks is usually not possible in physical systems, but with the careful design of network control and management

software, these primitives can be designed in to improve network resiliency. Also, especially important is the ability of a network to reconfigure adaptively in fractions of a second if necessary.

C. ARCHITECTING SURVIVABLE NETWORKS

1. Network Attribute Considerations

Architecting survivability into large, distributed computer networks draws on the disciplines common to the protection of critical systems such as security, safety, reliability, and fault tolerance (Ellison et al., 1999). The goal of designing survivability into networks is to preserve essential services that allow mission completion during network intrusion and compromise. Architecting the system to be survivable is a balancing act between the network's design to support the maximum functional capability under normal operations and the ability to defend against and recover from any compromise to the system while maintaining critical functions during attack and recovery. The success of system recovery is measured by the system's ability to minimize the consequences of degradation to system functionality and to the network's critical attributes by preserving data, and allowing the continued execution of essential services during an attack of the system. Critical attributes of a distributed network are the capability to access data and services and to share between network nodes, and to conduct the necessary computations and data manipulations to achieve the system's objectives. The challenge in architecting a survivable network is that during normal operation, it is desired to minimize the constraints placed on system operation and availability in the form of system defenses, but also desirable is the ability to have the necessary protections in place (procedures and countermeasures) to resist, recognize and to be able to recover from system degradation or failure, whether the compromise is due to system fault, unintentional accidents, or intentional attacks by intruders. The more survivable the network is, the greater its tolerance to threats and the lower the risk to operations.

a. Consequences

In architecting a network for survivability, the consequences to system operation and mission fulfillment that various threats have the potential to cause should vulnerabilities be exploited must be considered. This approach is slightly different than the classic models for risk analysis and assessment. While it is necessary to seek information about all known possible threats, where they might originate, the threat's capabilities, motivations, and timing to cause the network harm; keeping up with the multitude of constantly evolving threats, known and unknown, in the environment around the boundaries to a system can be an insurmountable task. New threats and threat tactics/methods emerge every day from global sources of unknown entities who would like to intrude on U.S. systems for various reasons. Since the universal set of threat agents potentially staged to cause system harm cannot be fully known, what is known and understood is used to examine it from the survivability (or consequences) angle. To do this requires looking at the network from an intruder's standpoint and examining how the network developer needs to architect the network to reduce susceptibility. In the areas where it is susceptible, an examination of ways to mitigate system vulnerability, and subsequently, the mechanisms and system characteristics is conducted to handle the consequences of a given attack and preserve critical attributes in the face of an attack.

b. Connectivity

Analysis of architecting for survivability is complicated by today's network systems, which because of their size, are unbounded (or an unbounded, networked system of systems of individual bounded systems). This is especially true of DoD's GIG from a top-level view. By its nature and global size, it is an unbounded system, much like the Internet (to which it connects). A network is unbounded in the sense that no single or group of participants are certain of who is part of the entire network. In an unbounded network, no centralized control exists, and participants have to trust the other members on the network to comply with agreed upon standards. Both legitimate users and threat agents act as peers on the net (Maier & Rechtin, 2002; Ellison et al., 1999). Obviously, without boundaries, a network's environment is now part of the

system. Threat agents come from the environment. Thus, they are intrinsically part of an unbounded system and can be thought of as latent participants (until they attack of course).

c. Control

Another complication to large, highly distributed networks is the constraint on network control and governance. When networks were small and bounded, their architectures were built around centralized governance that had a manageable span of control. One controlling entity had the power to enforce policy and enact sanctions for inappropriate network conduct. Network protection was implemented with static countermeasures, the most ubiquitous being firewall installations; first, at individual workstations, then in front of local area networks, and later enterprise firewalls were incorporated in the network architecture and integrated with the desktop firewalls. Changes and updates to firewall configurations were pushed to users by local system administrators or by a centralized network administrator (NSA/SNAC/IAD, 2006). However, this architectural arrangement is insufficient to protect systems as networks take on global proportions, with governance decentralized or non-existent, and the network characterized by interoperable and collaborative system of systems. Since control of distributed networks is so tenuous, there is good reason to consider network risk management from a survivability viewpoint. With an inability to impose controls throughout the entirety of the network, survivability architecture looks at consequence management, focusing on the mission accomplishment of network segments and on the creation of the ad hoc networks envisioned for the target GIG.

d. Governance

As the size and complexity of the network grows, operating standards and protection methods become schemas agreed upon by the membership of the network. When an organization makes the decision to move to service oriented architecture, the system takes on more characteristics of an unbounded network. A sophisticated architecture of countermeasures, authentication devices and procedures, and network behavior recognition and intrusion systems must be introduced, tested and monitored by

someone who has the responsibility for accomplishing the mission and ensuring the availability of services. Partitioned segments of the network can be loosely controlled (as is done with the Internet in countries desiring some political control), but even that governance and control is limited, and attempts to subvert it constantly occurs. The U.S. military's GIG has a better chance of providing some governance over its participants and its operations because, on a high order scale, the objectives of the participants on the grid are the focused around a common cause, and a form of constructive governance might be achieved. However, as the network users' objectives become more refined into distributed and parochial operational plans and tactics, this form of network control becomes more diluted, and governance of the net tends toward the problematic and control is less centralized. This fact soon becomes more apparent as the DoD lashes the individual services' network architectures together to create the global target GIG. The overall joint governance of the net most likely is based more on a set of collaborative standards rather than a defined rule set controlled by a central authority such as DISA.

e. Communication

In a distributed network architecture with services spread across many domains and an environment of diminished trust with no unified system administrative control, survivable network design relies on a common communications and routing systems to tie distributed services, diversity in coding and protocol mark-up, and node logic systems together in a survivable package. Since it is impossible to know everything about a threat agent, the survivable network requires an architecture built on the interactions between nodes such that protection is protocol-based instead of architected for a given network topology. The network must have some system of trust maintenance, and must have system-wide properties that do not reside strictly within nodes and is emergent and stochastic (Ellison et al., 1999). A functional decomposition of the networks attributes set the priority for where resources are allocated to protect and to recover those network attributes that must be maintained in the face of an attack, or must be instantly recovered because their function is time-critical, and any interruption would cause a failure of the mission.

The capability to maintain essential services (and maintain the associated essential properties) must be sustained even if a significant portion of the system is incapacitated. Furthermore, this capability should not be dependent on the survival of a specific information resource, computation, or communications link. (Ellison et al., 1999, p. 9)

2. Elements in the Architecture of a Survivable Network

a. Usage Models

To determine the make-up of a survivable network, the developer constructs a system usage model for the network, both from the standpoint of a legitimate user and also an intruder (since it was stated that they act as peers on the net). The usage model shows what services are essential and non-essential; the timing, load, and all possible uses of a network service (Ellison & Moore, 2001). For survivability, the architect must determine what survivability services are employed and their allocation. Survivability services and their components consider a threat agent's capability to access the network, to penetrate nodes of the network and systems on nodes, its ability to navigate within nodes to discover information, and the ability to exploit, or corrupt services in the node. Survivability services are as follows.

- Resistance to intrusion through the use of firewalls, diversity of programs, and encryption and authentication
- Recognition through intrusion detection devices, anomaly and behavior pattern recognition, trust maintenance, and self awareness methods
- Adaptability through backup programs, alternate connections, scalable bandwidths, learning from attacks, nodes share fixes with each other
- Recovery through redundancy and data/program replication, fault tolerant mechanisms, diversity in data storage

Since it is nearly impossible to tell the difference between users on a network, the only way to determine if the user is legitimate or hostile is to observe the user's behavior with respect to the system. Work on determining how to tell what differences in client behavior on a server can provide clues to illegitimate use of a network has been conducted by the Computer Science Department at Cornell University, among others. They have adapted the timeout feature of computer network fault detection to the process of transactions between objects and the timing of those transactions to

determine if a fault is real or just a transitory state of one of the clients on the network (e.g., entering or exiting the process during a transaction) (Birman, 2009). By virtue of its reliance on the service oriented architecture, the military's GIG network is unbounded. If a network partition is to be shutdown due to detection of a fault, the consequences of the shutdown need to be identified, the critical time of shutdown determined, how the data in a transactional state to be preserved, and what obligations are forfeited to the user or to the mission objective by network shutdown. It is most critical to recover the system before determining the cause because it often becomes apparent only during recovery, and not while in a shutdown state.

Architecting for a survivable network requires an architecture that allows no single point of failure, a system of continuous trust verification between nodes of the network, protocols that define knowledge between nodes, and specific services accomplished in a single node does not significantly detract from the network's overall mission should that node fail (Ellison et al., 1999). Work continues on determining where in the network layer the encoded trust information resident in the network's communication protocol can be interpreted, on what are the cost differentials with packaging server state information into protocols to verify trust and the availability of critical processes. Much research has been done at Cornell University, as shown in the description below, about work completed on recognizing errant network behavior, on the study of how network processes are ordered and how the network reacts when one process fails.

b. Fault Tolerance

One of the important aspects of recoverability in a survivable network is fault tolerance. This is the ability of the system to withstand failure and keep critical elements functioning mainly through the mechanism of redundancy. If it is desired to lower the risk of losing a critical capability, designing in a fault tolerant capability supports the systems capability to withstand attack and damage to the network and allows the continued access to critical services. Fault tolerance improves system reliability, availability, dependability, and safety. Redundancy in network components not only

protects the system from intentional attacks, it also improves reliability in the face of unintentional accidents and equipment failure. The key to fault tolerance is the ability to architect in reliability because “... in all practical systems, reliability is of great importance, and any system that is unreliable is likely to be unsuccessful even if it is safe” (Storey, 1996, p. 114). Here again, the emphasis on architecting a system for use and availability by increasing reliability is seen; one of the main drivers in availability, and balancing system and personnel protection with system utilization.

Architecting fault tolerance requires understanding the nature, duration, and extent of the expected fault. The nature of a fault can be random or systemic. Random failures generally are generally associated with hardware. Software most often exhibits a systemic failure because the software cannot become obsolete or degrade like a physical component, and software failures are evident in their specification, coding, logic, or variables. The fault duration can be permanent, intermittent, or transient. Many software faults exhibit an intermittent failure and it can be difficult to find the cause. The extent of a fault can be localized or system-wide.

To deal with faults and design fault tolerance, system models can be constructed to analyze failure modes and make an assessment of the effect of faults on the system given the nature, duration and extent. Hardware (especially computer memory and processing chips) is usually modeled with the “single stuck at,” “bridging,” or “stuck open” model of system operation, and analyzed with the Failure Mode Effect and Criticality Analysis (FMECA) method. These methods and models are important to analyze during the architecting of a networked system at the physical layer. As discussed in the section on risk methodologies, computer systems and network software faults are analyzed using fault tree analysis and its transposition, attack tree analysis. System software faults are difficult to detect as the test vectors for the software process can be overwhelming. Often software is assumed to have some faults, which are never detected and are tolerated. With this assumption, it is important that the system be architected for fault tolerance during design. It is far easier to discover and remove software faults during the development stage of the system life cycle than during operation. However, this method of fault coverage can become problematic under the open architecture

scheme that uses COTS components. The purpose of using COTS in system development is to take advantage of the testing already conducted by the commercial vendor, and to use their usage data during system operation for reliability determinations. Often, however, COTS software contains either proprietary programs or lines of code so large that it is prohibitive to double check the reliability of the program, or to ascertain if the software's coding is embedded with any malicious operators (Storey, 1996; Anderson & Hundley, 1998).

Open architecture is one good reason to build in fault tolerance. The other is to mitigate the effects of an attack on the network, and to support system recovery by architecting the system to be survivable. To build in fault tolerance, the system is designed with redundancy. However, the redundant design has to be smart. Limited by resources, bandwidth, power, space, or the environment in which the system operates, a system presumably cannot be made with an infinite amount of redundancies such that it contains an infinite set of duplicate components with which to switch over. Additionally, for systemic failures, a redundant component of a component with a systemic failure also fails the same way and is redundant in the true sense of the word; not necessary. For systemic failures, the redundancy needs to be diverse so as not to duplicate the systemic error in the primary component. The architecture of the redundancy is also determined by whether the system is composed of hardware, software, information, or time.

- Hardware is classically made fault tolerant by triple modular redundancy; three components that perform the same function and are switched on or off by a fault sensor, or have their outputs auctioneered to select the component with the valid output.
- Software programs can be duplicated to produce the same output but by a different process to eliminate system errors in the program. For an attack on the network, it is necessary to ensure the backup program is in a different location and cannot be corrupted by the same threat agent that corrupts the primary program.
- Information is made fault tolerant by duplicate repositories of data, stacking information on top of the data to ensure its validity such as check sums or indexing schemes such as hash functions and tables.
- Timing functions for program execution can be used to ensure a fault tolerance from intermittent failures such that the program or service is timed to execute when the process fault is recovered. There are many

timing schemes for program execution operating or underdevelopment such as cloud computing and multicasting programs (Birman, 2009).

Once the architecture of the redundancy has been determined, it is necessary to architect the system for fault detection. For network hardware, the simplest arrangement is called masking, which does not actually detect a fault, and basically allows a redundant system to pick up the load. Dynamic systems sense faults by examining output and comparing it to a desired output. Upon fault detection, the system switches to a redundant component to contain the existing fault and reconfigure the system for continued fault-free operation. There are many arrangements to architect the system for fault detection and tolerance, but a detection system inserts another component into the system that must be analyzed for its reliability to not let a system fault go undetected. Obviously, redundancy in detection components should reduce the risk that a valid fault may be missed or a false detection of a non-existent fault induces unnecessary action.

Software fault detection is complicated by the fact that faults in software are always systemic. As mentioned above, architecture for fault tolerance in software is achieved by diversity, or what is called N-version programming. Several versions of the software run concurrently on one or more processors, and their outputs are compared for similarity. With only two versions, if a difference is detected, it is difficult to tell which version is correct, so the system must perform further diagnostics to determine the correct version. The other software detection scheme, called the recovery block (Storey, 1996), is to run diagnostics continually on all program versions to check for issues such as run-time errors, math errors or reasonability. However, to make a software system fault tolerant, the system needs to recognize and fix a system state condition. To detect a fault, a fault must occur. In software, the faulty execution changes the system state before the redundant program assumes control. To fix this situation, the state of the system before a failure needs to be known and saved somewhere so the system can recover. Much research is being conducted on ways to save and reset system states without having to make a copy of system states continuously. One example is the new multicasting technique over a layered network. Markov non-time dependent models of the system state can be used to determine the risk due to a software fault (intentional intrusion), and

can be used to inform the architecture of the system to control the component and sub-system state changes and recovery to the operating state. Software reliability predictions can be difficult to assess since some parts of the software are used infrequently, and a fault to an intermittently used portion of the program may not show a fault for quite a while into system operation. For this reason, testing of all possible program execution cases is important, and if too many cases exist to make it economically feasible, a test and verification of those executable programs, which impinge on critical operations, must be tested.

D. SURVIVABILITY MODELING

1. Reactive Risk Analysis

Reactive risk analysis (Hamdi and Bordiga, 2005, pp. 783-785) examines the resilience of a network once an attack is underway by analyzing the network's reaction to the attack given a set of attack detection devices and countermeasure mechanisms to resist attack and recover the network. The reaction to the attack depends on the following.

- The type of attack (from attack tree analysis)
- The number and type of intrusion detection devices and their efficiency at detecting true intrusions and ignoring false alarms
- The number and type of countermeasures installed and their capability at resistance and system recovery

A consideration in deciding how resilient to make the network is the cost of detecting and reacting to an attack weighed against the benefit of detection and reaction. The benefit is highly dependent on the capability retained and the functionality or data saved or recovered, and the effect of the loss before recovery on the ultimate objective of the network at the time of attack.

An intrusion detection system (IDS) is most often composed of a sensor and an analyzer. The sensor uses either pattern or behavior recognition to tell that an unauthorized node has penetrated the network and alerts the analyzer to attempt to capture the intruder's parameters (packet header fields and other metric data). Upon

inspection, the analyzer makes the determination from the captured data whether or not this is an intruder so that the other countermeasures can take appropriate action to resist the penetration, and recognize and recover any lost data or functionality.

The authors developed a cost/benefit model that could be used to conduct an analysis of different types and levels of IDS and countermeasures to support the decision of how resilient a network should be given the level of funding and other resources available. The model formulation is expanded in Appendix C. One unique factor claimed by these authors is the use of an attack progression factor in the analysis. Depending on the type of attack, the impact of an intrusion can be constant or can grow linearly or exponentially over time as the intrusion progresses. How the attack is countered and the resource costs to deal with the intrusion depend on the characterization of the initial impact as well as what effect the attack has over the time the attack is active until it is stopped and system recovery has been initiated.

The four elements of the reactive model are as follows.

- Cost of detecting the attack
- Cost of reaction
- Impact of the attack (when the progression factor applies)
- IDS efficiency

The utility of this model is helpful in an analysis of the costs of IDS and countermeasures from a comparative standpoint if it is possible to come up with plausible values to insert into the model's variables. While the progression factor is an interesting and expanding concept for the model, determining an expression or function that captures all the dynamics of the progression of an attack is probably not realistic.

2. Modeling the Recovery Phase of a Survivable Network

Heegaard and Trivedi (2009) develop a model to quantify the survivability of a telecommunications network by examining the virtual connections state and capacity between peering nodes to maximize throughput and minimize delays when the network is under failure from intentional intrusion, natural disasters or failed states. Their approach to the steady state model is similar to a model done by Chen/Garg/Trevidi. that looked at

rate of frame drop in steady state and transient losses due to faults in a wireless ad-hoc network (Chen, Garg, & Trivedi, 2002). They combine a continuous time Markov chain (CTMC) model with traffic queuing models for the steady state network availability. Then, they use several different models for propagation of failures due to undesirable events and quantify the network's recovery cycles.

The authors contend that making a network more survivable is accomplished by three actions; i) preventative measures (stop the attack before it starts), ii) designing in enough spare capacity and sufficient diversity to make the network fault tolerant, and iii) developing and configuring proactive and reactive traffic management techniques and protocols (equally applicable to data networks and wireless networks as traffic management is a vital attribute of any efficient network). These models' utility is best captured in the risk and survivability analyst by informing the analyst possible network attributes and software functions that pose a major impact on survivability and where to place an emphasis on designing in a more robust survivability capability such as improved data replication or diversity of components.

The Heegaard and Trivedi model quantifies the virtual management of network traffic for survivability and discusses how it is accomplished with changes to traffic routing requirements, traffic loads, and capacity changes due to random, non-synchronous service requests. The undesired events cause failures to nodes and their communication links (arcs between nodes), which reduce network resources of bandwidth, memory, and processing speed and capacity. Recovery is accomplished through rerouting and restoration of the failed nodes and links. That these models are being considered by design engineers supports evidence that efforts to design traffic management techniques to improve survivability in networks are plentiful. Work continues to improve on the techniques of traffic and process flows through different layers of a network as is being done in work at Cornell University on a "Virtual Synchrony" process. This technology uses the multiple processes handling of the Client-Server Object Request Broker (CORBA) middleware in a fault tolerant architecture on top of multicasting techniques of network traffic management (Birman, 2009).

3. Characteristics of Dynamic Mobile Networks

In their work on describing and simulating dynamic mobility networks, Scherrer Borgnat, Fleury, Guillaume, & Robardet, (2008) look at how networks change over time with new nodes attaching and failed nodes being removed from a network. Through analytical models and simulation of a mobile communications network attached by Bluetooth®, they concluded that link creation and deletion is independent of one another and can be modeled by a Markov process, but the interaction within the network is random and characterized by the creation of communities that intensify the data flow rates within the communities at statistically insignificant and non-correlated ways, which complicates the modeling of the network flow traffic within a large-scale system. Since the activity of communities changes randomly over the temporal scale, a true measure of information loss probabilities is difficult to simulate, whereas link creation and deletion can be formulated and simulated. That communities have unpredictable data flow rates and link connection creations between them seems intuitive as human activity that requires a network to control an event or meet a schedule most times relies on external events independent of the network's activity level or its steady state processing of information.

E. SUMMARY

A network designed for survivability and resiliency is one that can continue to provide critical services while under attack and has enough resistance and adaptable recovery to return to its normal state. Survivable networks are architected to recognize an attack, resist the attack to the greatest extent possible and recover quickly after the attack has been stopped or thwarted. Networks designed for resiliency are capable of immediate adaptation, shifting the workload in the network from the failed modes to the operable nodes with little or no effect on the end-to-end capability of the network. An example of resiliency in a network is the adaptation of Unmanned Ariel Systems (UAS) to pass surveillance missions between sensor platforms when they are networked with a resilient

middleware communications package, allowing uninterrupted intelligence to flow to the field unit depending on it (deJong, 2009). A survivable and resilient network provides defense in depth for the operation of critical network systems.

Survivability is scenario-driven, and defining survivability requirements with which to build a survivable network system is challenging. For this reason, the architect must look at the network's boundaries, the interface to other networks, and define where the line is drawn to resist attacks from threats that come in various ways with an array of capabilities. Once an attacker has penetrated a network, the architect must look at the capability of the system to adapt and recover while stopping the attacker's progression. Adaptability has to be built into a system on initial design. Unlike manned systems that can adapt with human intervention, network systems require adaptation in fractions of seconds, through complex software logic and must be able to do this automatically.

Quantitative models of network operational characteristics and attributes are informative for measuring a network's capability to adjust one parameter under failure from a single attack scenario. When designing a system for survivability, these measurements may be useful in the evaluation of tradeoffs between different system architectures as long as the parameter under study is reflective of a quality required to be maintained in the network during attack to ensure mission objectives continue to be met.

Some conclusions follow that can be made with respect to survivability modeling.

- The ability to quantify the survivability of a network is an important step in determining the reliability and availability of a network under attack. As the network grows in size and complexity, quantifying survivability becomes quite complicated as the conditions and constraints on the model become more detailed and interdependent.
- The models above are not process models per se but are system models that formulate the problem of survivability mathematically or systematically and can be used to solve for a quantitative number representing survivability by optimization techniques, probability calculations, or simulation.
- The first step in quantifying survivability of a network is to determine the characteristics of the network under normal steady state operation. The classic model for steady state network node characteristics is a continuous time Markov chain, with information arriving at a node in a Poisson distribution and service through the node processing in an exponential

distribution. There are many situations where the assumption of these distributions is not accurate enough to provide a reliable representation of the network's operation, and care must be taken to understand the information flow characteristics within the network, how they are changing over time, and the most accurate depiction of the network's handling of information from sender to receiver.

- Survivability does not consider the probability that an attack is made on the network; the attack has already commenced, and the analysis of survivability deals with how the network handles the attack once it has begun.
- Survivability analysis must balance the costs of designing the system for survivability with the cost in functionality reduction to implement survivable features. Some survivability features have direct costs of technology development and installation, monitoring, and maintenance, but does not have an opportunity cost in lost functionality as the countermeasure does not inhibit normal operation, such as an intrusion detection system (IDS) or device, although one opportunity cost that might arise from an IDS is the reliability of the IDS to minimize false alarms. Other survivability features may involve an opportunity cost as in traffic management schemes, which lower throughput below that which is capable without this feature. A direct cost may be incurred if throughput functionality is important and traffic management restrictions are mitigated by larger bandwidth. Paramount should be the cost of losing capability in an attack scenario if survivability is not designed into the network, and the risk of losing the network's capability for an unacceptable period of time because recovery and rerouting were not designed into the network in the first place.
- Quantification of survivability requires the measurement of some network value of interest (packet loss rate, delay in packet arrival). The formulation of the model must have a basis in truth or in experimental data to back up the assumptions as to how the changes in these key parameters are affected by a network failure from attack.
- Network configuration and network operating characteristics change depending on the applications being used, the number and connectivity of network members accessing services or communicating with other members. While node behavior can be predicted on knowledge of the node's make-up and what the node is designed to process or pass, the behavior of the members can be random and unpredictable. Survivability must take into account the user population and the typical behavior patterns of the typical user and how that behavior might change based on the external environment to which the user is exposed.

Obviously, models that assist in quantifying a network's survivability support management of risk to a network. However, what models like these do not provide is the answer to the question of what value of survivability is required to meet the mission. Proceeding to the next step, a detailed mission description must be articulated that specifies the parameters a network must meet during network failure recognition and recovery. Without a clear-cut mission effectiveness requirements and specification, the capability of the network to survive a given attack is meaningless. For instance, in the Chen & Trivedi wireless network model, survivability is the capability of the network not to lose too much information from the sender to the receiver and to have them communicating once again as quickly as possible. However, it has not been determined what the minimum values of packet loss or of packet delays required to accomplish a given task, or what the task profile for the network is. Survivability analysis must include a definitive description of system's goals. For instance, in a commercial wireless telecommunications network, it would be helpful to know the necessary recovery time needed to keep from losing too many customers due to dropped calls and the probability that the network is able to meet that minimum network service quality under attack from the most likely threat or the most likely failure. Also not specified in the model is what information is lost; or is there a priority in information content that dictates what can be dropped and what must make it through the network? If the network drops a connection for only a minute, the information lost may or may not be important, but it is not possible to tell from these models or to quantify that attribute. While the models represent the system well under a given attack, most network models use the dropped link or failed node as the basis for model development. Other problems could be inflicted on the network such as the rerouting of sensitive information, or the distortion of information without sensing a connectivity problem, which would prompt a node switch. It is unclear how this situation would be handled by these models. As the number of types of threats increase, the solution to the optimization problem becomes quite complex.

VI. CONCLUSIONS

A. SUMMARY

The Department of Defense and the military services are well on their way in establishing information dominance enabled by network connectivity as the centerpiece and dominant factor in the defense and warfare strategy of the present and future. The edge over the enemy is the ability to control events through knowledge of the situation, eliminating as much as possible the “fog of war.” It is essential that this information be shared with the war fighter in as clear and unambiguous way as possible; certifying that the information shared gets to the war fighter, is the correct information, and that it is unavailable to the adversary. It is equally important that the opposition be hampered as much as possible in its ability to reach this goal with their war fighters. The desired effect is to increase the density of the enemy’s “fog of war.”

The DoD CIO says: The Department of Defense is transforming to become a net-centric force. This transformation is based upon the recognition that information is a critical strategic component that enables decision makers at all levels to make better decisions faster and to act sooner. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it is at the heart of net-centricity. (DoD GIG, 2007, Preface)

The U.S. military’s information systems and the network enterprise are threatened on several fronts; equipment malfunction, unintentional mistakes and accidents causing system and network inoperability, hazards from natural causes and the exposure of systems to hostile environments, and intentional disruption and destruction of data and functionality by many adversaries, each with their own motivation for opposing the military’s objectives and disrupting the flow of information.

The GAO warns: In addition, DOD faces risks inherent with the nature and scope of the effort it is undertaking, for example, risks related to protecting data within the thousands of systems that will be integrated into the network. Furthermore, the technical challenges to develop new networking and network management capabilities to support mobile, integrated communications are considerable. (U.S. Government Accountability Office, 2004, p. 4)

Much effort since the start of the information age has gone into research, development, and testing of technologies and practices that increase the security of computers and networks. The need for an ability to recognize the threats to information systems and networks and to determine what to do about the threats is paramount. This is best accomplished through a robust program of network and information system risk analysis and management. That it is important to take the holistic view of network risk assessment rather than focusing on short term fixes is clearly articulated by Chittister & Haimes in their article on Cyber security and the software lifecycle.

The balance for achieving secure information systems is tilted more toward short term tactical measures, focusing on fire walls, patching, and response to cyber attacks, and less toward long-term, strategic approaches that address the entire software lifecycle development. (Chittister & Haimes, 2006, p. 2)

1. Network Architecture

This thesis examined a network's architecture from the hardware aspect (topology) and software (layers and SOA) and how certain architectures create or mitigate vulnerabilities that could be exploited by threats.

Conclusion 1: A study of network topology from the standpoint of vulnerabilities should be part of the decision in the evaluation of alternatives along with performance and cost. Networks architected from concept definition to resist attack are more capable of evolving with the growth of the network into a more secure posture.

Conclusion 2: The decision to use open architecture and to take advantage of the attributes of a SOA carries with it several implications that can introduce vulnerabilities. One of the principle sources of introducing vulnerabilities through software architecture is the open architecture and SOA reliance on COTS. COTS software may be questionable as to the testing conducted before use in the military's network systems in addition to the possibility that there may be hidden software programs or logic that can introduce unknown vulnerabilities that can appear during network operation.

2. Network Risk Management

The thesis researched the elements of risk, especially as they apply to networks; the composition of a risk management process, with a detailed look at DoD's risk management for acquisition programs, and what attributes of commercial risk management processes might support the continuing improvement of a network enterprise risk management approach for DoD Net-centric operations and the GIG architectural framework.

Conclusion 3: Identified risks need to be fully assessed for the potential not only to disrupt the network, but also the consequences on the operations they are designed to support. A rigorous and enlightened assessment of network risk should support network designers and operators in making a decision as to whether it is worth the cost in funding or opportunity to plan and implement a mitigation strategy for a given risk. The answer to the question "What is this mitigation strategy protecting?" has a direct effect on the mitigation strategy employed.

Conclusion 4: Attack trees are a useful tool in analyzing network vulnerabilities and assessing the motivating factors of threats to attack a network. When analyzed from the standpoint of game theory, attack trees (based on the reliability analysis done through fault trees) contribute to the insight of network vulnerabilities as viewed by the network versus by the threat.

3. Network Survivability and Resilience

This thesis examined resilience and survivability of networks and strategies for architecting networks for those qualities. Survivability means a reduction in susceptibility and vulnerability, and the ability to recover. Resilience in a network is an abstract quality that metaphorically means the ability to resume the previous shape. Architecting a network for resilience is challenging in that the requirements for survivability are scenario driven. Articulating and defining a survivability or resilience requirement can be problematic.

Conclusion 5: To architect resilience into a network, a network architect must look at the network's boundaries, the interface to other networks, and define where the line is to be drawn to resist attacks from threats that come in various ways with an array of capabilities. Once an attacker has penetrated a network, the architect must look at the capability of the system to adapt and recover while stopping the attacker's progression. Adaptability has to be built into a system on initial design.

4. Network Enterprise Risk Management

This thesis compared some of the popular risk management processes in the public domain. It examined how their methodology might support DoD's network enterprise risk management process to achieve a survivable and resilient enterprise network and support DoD in making risk assessments and decisions on the cost/benefit or value of the choices in alternative architecture and countermeasure use for risk mitigation implementation.

Conclusion 6: This thesis contrasted some of the popular risk management processes in the public domain. A common thread in all the commercial process models is the necessary involvement of the entire organization in the process, from top level management to the network administrators and functional managers. Leaders and the people in command positions need to take an on-going role in the security and risk management of their most valuable assets, the networks and the information and functionality contained therein. Risk management is a continuous process.

Conclusion 7: In the end analysis, managing risk is a balancing act. However, it is a process that is necessary; it is a process that needs to evolve; and it is a process that needs to be continuous. Risk could be eliminated by erecting barriers to impenetrable potential threats, or by just shutting everything down. The consequence of this action is that network users would be unable to use the network to achieve their objectives. The converse is to ignore the level of risk or setting the criteria of an acceptable level of risk too low to avoid mitigating it; allowing uninhibited access and mobility to data and functionality contained in the network. This method is just as untenable as shutting down the network completely every time the network is attacked. Without mitigation, the

network would be inundated with illegitimate members intent on causing harm to satisfy many motives (data destruction, fabrication, and interruption of critical services). The process of managing risk gets more complicated as systems grow in size and complexity, and as the systems become distributed both in functionally and geographically. The answer is to conduct a continuous assessment of the risks to a network, to balance network capability prudently with network security, and applying the available resources with which to do that wisely.

B. RECOMMENDATIONS OF AREAS FOR FURTHER RESEARCH

It is the contention of this thesis that to continue to provide the network capability desired in the GIG enterprise to support the strategy of information dominance even when the network is under attack, the network must be designed with the quality attributes of survivability and resilience. Service Oriented Architecture, with its loose coupling at the boundaries and its objective of software reuse by making the service independent of the client through the use of description language and callable interfaces, offers an opportunity to examine this process for ways to make the underlying network resilient and adaptable to realigning the service when the network is under attack. Further research and analysis should concentrate on how this would be done.

Service Oriented Architecture offers significant advantages in an enterprise as large as the GIG is envisioned to become. However, one of the biggest sources of vulnerability that increase the level of risk to the enterprise is the use of COTS software in designing the network with open architecture. Considering the cost savings and time to provide capability to the war fighter through the use of COTS, research and analysis on how to close the vulnerability gaps created by using COTS should be conducted. The use of quality control measures such as Capability Maturity Model Integration and others is vital to closing that gap. Determining sufficient software testing requirements that do not take an inordinate amount of time or resources but still provide the assurance of quality would be a step ahead in the military's ability to enhance the one factor that is under their control in the risk equation; i.e., reducing network vulnerability in a network that provides invaluable resources to the war fighters in their efforts to reach their objectives.

THIS PAGE INTENTIONALLY LEFT BLANK

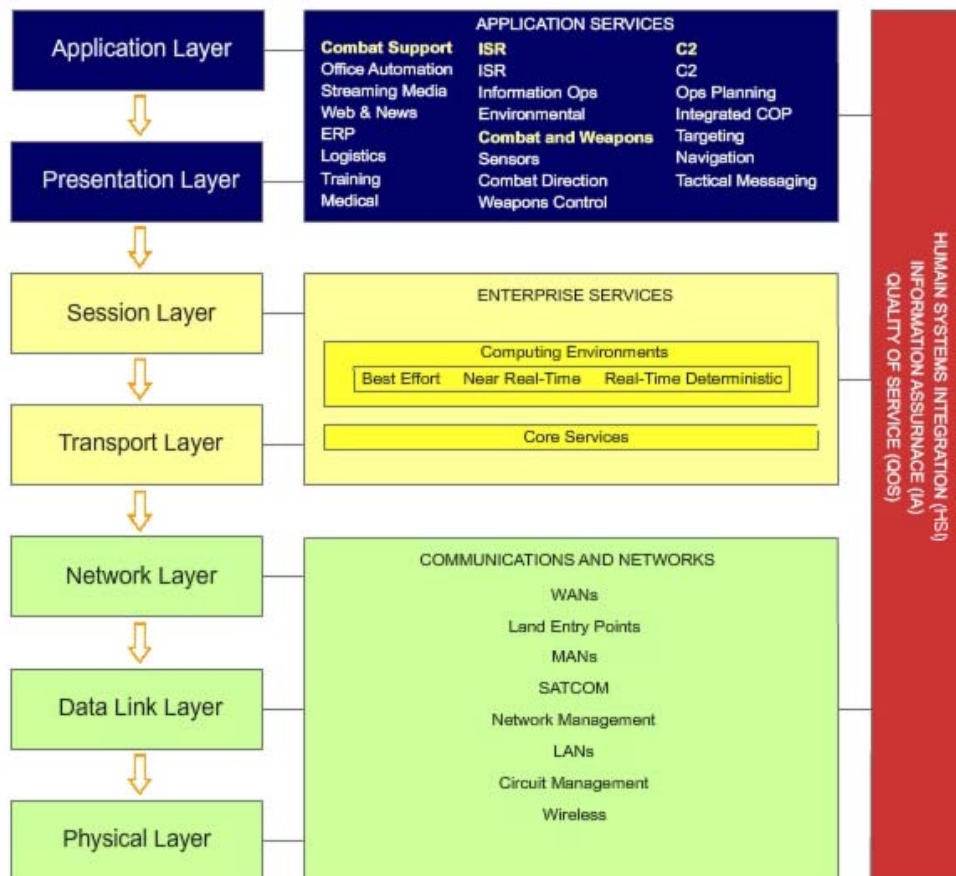
APPENDIX A. VULNERABILITY AND MITIGATION STRATEGIES BY NETWORK LAYER

A. INTRODUCTION

As discussed in Chapter II, a network is a complex organization of physical components and connecting devices arranged in a certain topology, signal paths, software logic controlling the signals, protocols which define how information is packaged, logic programs controlling the routing of the packets of information, packet addressing schemes to obtain the information from source to destination, software programs for determining who receives what information, mechanisms to keep packets from interfering with one another, the data and functionality contained in packets sent through the network, and a variety of other schemes for making the network operate correctly and perform the functions desired. The International Standardization Organization ISO has decomposed the operation of networks into seven layers in its Open Systems Interconnection (OSI) model, and by in large, a plan to evaluate and mitigate risks to network enterprises must consider the layer abstractions to define the mitigating strategy properly that is to be used for the security software logic and mechanisms to operate correctly. The boundaries between some of the layers can overlap, and indeed network abstractions by other organizations may combine ISO layers in their definitions. For instance, Figure 17 shows how the Navy has combined layers of the ISO model into three layers in its model of FORCENet; the communications and network layer, enterprise services layer, and the applications services layer. In this discussion, a comparison is made between the different layers of the ISO Open System Interconnection (OSI) model layers for vulnerabilities and the Quality of Service attributes that need protection.

This figure is a comparison of the network information abstract as depicted in the ISO seven layers with the layers defined by the U.S. Navy's FORCENet model of information extraction. A mapping of the vulnerabilities and mitigating strategies can be made into the FORCENET model from the description of the specific layer in the ISO

model. While the mapping is not necessarily direct, as these abstraction models overlap in their actual functionality in an operable network, a comparison can be made and translated between the two models closely enough to have some utility.



The risks inherent in the ISO layers translate into the FORCENet model to inform the Navy's network development team the types of risk to look for in each of the three layers of the FORCENet model.

Figure 17. ISO Network Layers Mapped to FORCENet Network Model (From: Stewart, 2006)

B. NETWORK ISO LAYERS AND THE RISKS TO NETWORK QOS ATTRIBUTES

1. Physical Layer

Description: This layer is defined by the hardware of the network, the devices that constitute a computer workstation or central processing unit of a controller, memory units

(hard drive, compact disc driver), network interface cards (Ethernet, modem, SONET token), electronic switching devices (hub, switch, router), connection hardware (Fire Wire, Universal Serial Bus, Bluetooth,), connection media (optical fiber, twisted pair cable, wireless radio signals), and power supplies. The hardware devices of the network are constructed to prevent collision of data, to provide multiplexing, and to form the electronic signals in the shape required for the communications medium (packets for wired systems and frames for wireless signals) (Smith, 2003).

Vulnerability: Primarily, the threat is to the network's availability by physical damage to components as well as the reliability and availability of hardware components. The threat at the physical layer is probably as likely to come from an unintended accident (component assembly or proximity to a hazard) as from a malicious attack. Interruption to power sources can cause damage to sensitive electro-magnetic components through electro-magnetic interference or power surges.

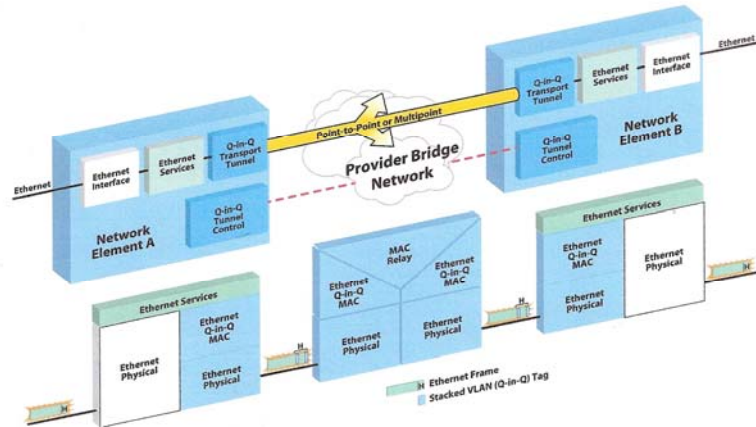
Mitigation Strategies: As in other hardware systems, availability can be enhanced by fault tolerant strategies of redundancy and diversification. Physical separation of components at this layer is advantageous as well as power isolation techniques such as surge suppression. The selection of hardware components and their location in the path of the network also affects the ability of the hardware to resist attacks. Speed of transmission and bandwidth of the communications medium affects the ability to get volumes of information to the right place within a time specification. The physical layer is the first step in the architecture choices of a system since the components chosen to do certain tasks, the quality of the hardware, and arrangement of where they are connected, what physical connectors are used, what shielding of cabling is employed; and many more architectural choices drives the cost of the network. It also determines the nature of the subsequent layers and what software can reside on the system components to perform the services architected in the upper network layers.

2. Data Link Layer

Description: In this layer of a network, electronic signals are passed indiscriminately node to node by frame delivery. These are the signals and packets that are transmitted through the physical lines (or through the air in wireless networks) by data link protocols such as ANSI standards of connectivity 802.2 and 801.11. (NSA/IAD, 2005). This is the layer in which the Media Access Control (MAC address) number is assigned to a particular piece of hardware, the internal addressing of a local area network. Basic protocols (rules) for sending signals from a node or workstation like the multi protocol label switching (MPLS), Ethernet protocols, token ring, and point to point protocol. In this layer, the network conducts logical link control (flow control) with flat addressing of information packets (Smith, 2003).

Vulnerability: Since this layer is merely the flow of information packets before they are guided by source and destination programming, the availability of data and services is the QoS most threatened at this layer. However, data signals that flow through the Internet can be intercepted because of the availability of access for anyone that can connect to the internet. Thus, packets (or wireless data streams of frames) could be intercepted, and if not encrypted, could lead to loss of confidentiality.

Mitigation Strategies: Since encryption of data is not done on this layer, the technology of service-transparent transport or “tunneling” is normally employed to protect the data streams using Ethernet technology. It can be implemented in this layer or in the physical or network layer to shield the data stream from recognition upon interception. Figure 18 shows a typical tunneling architecture using Ethernet technology and control and management functions (May, 2004). In addition to tunneling, data replication at this layer can provide some mitigation to availability of services.



Tunneling is a method to keep data safe while in transit outside the security protections of the Local Area Network when it is between source and destination gateways.

Figure 18. An Example of Tunneling at the Data Link Layer with Ethernet (From: May, 2004)

3. Network Layer

Description: The network layer in a network is the abstraction that implements end-to-end packet delivery and routing through a network with addressing via Internet Protocol (IP). It is also the location where network management services are conducted such as how the packets are handled at each intermediary node (usually a router). Packets are sent from the source without establishing a connection with the destination, and routing is done through subnet routers for message forwarding and data flow control. However, the source can receive acknowledgement, and some error checking and control of the packets is done at this layer. With hierarchical addressing being done in the network layer, this abstraction defines the path which the packets take to reach their destination. The network layer can make service requests to the data link layer (Smith, 2003).

Vulnerability: Since this layer is where the network management takes place, the configuration, and performance of network traffic flow is monitored and managed from this layer. This is also a layer where access control is maintained to network system components; those components that manage network characteristics. At this layer, intrusion into the network affects network performance characteristics such as

connectivity between critical nodes, how traffic is routed node to node and number of hops from end-to-end. This also affects the latency of data travel, and on software control of bandwidth allocation to certain users, subnets or LANs. Availability of data due to connectivity issues or routing issues on the network layer is the major threat. Integrity of data can also be affected, as intrusion into network management can cause excessive information packet loss and distortion of data received by the end user.

Mitigation Strategies: Maintaining minimum configuration standards for the network and components, especially routers, on the network is important for maintaining security to ensure availability of network paths for legitimate information flow. To assist in security management, it is in this layer that intrusion detection device characteristics are abstracted to measure their performance in detecting unauthorized access to the network. With basic packet addressing at this layer, name conventions and protection of network addressing is important and confidentiality network component locations are maintained by hiding Domain Name Servers (DNS) behind an encryption and authentication device and preventing DNS reverse look-up that gives a domain name away. When the packets with an IP address leave the LAN, the IP address can be repackaged to prevent IP spoofing. Spoofing is a way for malicious actors to use someone else's IP address notation to gain access to an unauthorized location.

4. Transport Layer

Description: The transport layer abstraction is where the information and control packets have been fully addressed with transmission control protocol (TCP) or the universal datagram protocol (UDP) and prepared for transmission from one user to another. TCP is a connection-oriented protocol. Port numbers are added to the IP address to allow access to ports called network sockets. The TCP addition to the packet address establishes the communication between sender and destination (or host and application). Additionally, packets are assigned ordering numbers to allow sequential reception and reordering at the destination, and it allows the ability to resend packets lost in congested nodes. At the transport layer, the network seeks to provide congestion avoidance. Between TCP and UDP, UDP has a higher throughput, which means a shorter latency

and is often used for video and Voice Over Internet Protocol (VOIP) where data drop is acceptable, but reduced latency is desired. The Hyper Text Transmission Protocol (HTTP) uses TCP for web browsing (Smith, 2003).

Vulnerability It is in this layer and the network layer below that the distributed denial of service (DDoS) attack is launched. With the ability to address IP packets fully with TCP addresses and port numbers, the attacker can target a network component for flooding with traffic from commandeered workstations called “robots,” and the attacker sets up a network of these robots to establish a “Botnet” that then causes an overflow of requests for service through a legitimate network node.

Mitigation Strategies: This layer protects information mainly through the establishment of virtual private networks, an arrangement of nodes in a physical network authorized to communicate and pass information end-to-end. The VPN is established by node authentication through security procedures such as password recognition and firewall installations. Another technique to controlling the direction and path of information through a multi-node network is to establish network overlays where only certain nodes accept signals and packets of a certain type (for instance differentiating light wavelengths in optical fiber). In addition to the software tools that provide a secure socket layer or SSL (a program to control a user’s ability to “plug in” to a network) for guarding port numbers so that an engineered TCP address cannot be constructed, an effective mitigation to the DDoS is the adaptable router reconfiguration, aided by behavior and pattern recognition software in an intrusion detection device to sense when unauthorized service requests are in-coming and block them. Another tool that can be used to control network participation is addressing packets with secure IP (IPsec).

5. Session Layer

Description: The session layer handles requests and response between applications or hosts. The software controlling actions in the session layer handles the setup and management of sessions. In this layer, authentication and permission is controlled. Sessions management software tries to reconnect the original connection path through the network when a connection is dropped (Smith, 2003).

Vulnerability: If the sessions management program does not verify the authorization of a user to set up a connection with an application, database, or other user (say for collaboration), information could be stolen or altered, affecting information integrity and confidentiality. In addition, an unauthorized member in a network could repudiate the information sent by a broadcasted, thus causing delays in successive information being sent by the need to resend information continually that was received the first time.

Mitigation Strategies: It is critical in this layer to gain authentication of those users accessing a session with an application or service so that information remains confidential. Security software programs that provide authentication and access control are important to keep the session from being disconnected or from information being hijacked by an unauthorized member of the session. The session and transport layers are where software called middleware resides in a network system. Programs have been built to control who is in a session, who can send and receive information, and how information is broadcast through the virtual network created by the session. Transport and session are the ISO layers that are aggregated in the FORCENet model above as the enterprise services layer. Network management programs designed in the Common Object Request Broker Architecture (CORBA) are resident in the session layer and determine who is able to retrieve what objects (complete programs or sets of data). Middleboxes are the components that comprise the middleware in the sessions layer. They use programs such as the Network Address Translator (NAT), load balancers (rewrites packet headers), (Joseph & Stoica, 2008) and intrusion-prevention devices as a type of firewall at the interface between applications and the network. (DISA, 2009; NSA/CSS, 2009). Service Oriented Architecture often uses a Distributed Data Services architecture in developing programs which are based on a data-centric model to establish a loose coupling at the middlebox interface with the network versus an object model that tightly couples the source node with the network management structure and the network operating system (Joseph & Stoica, 2008).

6. Presentation Layer

Description: In this layer, data packets are assembled into language recognized by the program using the data it has retrieved from the network and it is where data sent from a program is packaged into packets for delivery through the network. Encryption of data is usually performed in this layer, but can wait until subsequent layers before transmitting the transparency of the network (Internet). EXtensible Markup Language (XML) is a method for packaging data sent from one program to another with a different language (NSA/CSS, 2005; NSA/CSS, 2008). Extensibility is the quality that allows add-ons to permit the evolution of the packaging to grow with changes to network configurations, network control procedures and development of new applications. (Smith, 2003)

Vulnerability: Data integrity and confidentiality is at risk in the presentation layer since access into this layer puts a malicious actor in contact with data or programs before encryption. On the other side of the interface to the sessions layer, if data has not been encrypted and marked up in accordance with an organization's security policy (security tokens, digital certificate, and userID/password pair), the data is available for pilfering and/or corrupting.

Mitigation Strategies: To provide security to the markup, XML has variants that attach onto the XML standard data representation. Used for web services security, Simple Object Access Protocol (SOAP) supports digital signatures and encryption and forms the shell to carry security tokens, Security Assertions Markup Language (SAML) and other security headers attached to the data. Extensible access control markup language (XACML) allows the inclusion and encapsulation of security measures on data packets within the construct of a security management and services architecture. XAMCL executes organizational policy models on information packets from the Attribute-based Access Control model (ABAC) and Role-based Access Control model (RBAC) to the Identification-based Access Control model (IBAC), Authentication-based Access Control model (NBAC), and Authorization-based Access Control model (ZBAC) (NSA/IAD SOAP, 2008). The last of these is compatible with a data-centric security model where the data and the network owner are kept separate, making this type of XML

packaging security system compatible with the goals of Service Oriented Architecture and the capability to share information securely across very divergent platforms. Further protection of data can be done in this layer (before markup in XML for transmission over the network) using “hash tables” (Walker, 2008).

7. Applications Layer

Description: The top layer of the ISO model of abstraction is the applications layer. This is where the services are performed. Many standard protocols are used in the applications layer to allow access to various services. The more common protocol which allows applications to access specific services is HTTP (NSA/SNAC, 2001). In the applications layer, the network has finally reached the point where processing power is accessed, data is stored, and real-world input from things like sensors or the human interface are translated into digital format in the language used by that processor (Smith, 2003).

Vulnerability: The applications layer is where received data is processed to be delivered to the physical interface (e.g., display) and control of outgoing data from storage or a physical interface (e.g., keyboard) is manipulated for subsequent transmission through the network. Since data and programs have been unencrypted for use by the end-user at this point, data and programs are highly susceptible to interception, and theft or fabrication. If a malicious actor can reach this point, integrity and confidentiality of information is easily manipulated for retrieval by the attacker or by the attacker modifying incoming or outgoing information.

Mitigation Strategies: If, in a collaborative session, loss of confidentiality to information might be mitigated if the end user has a way to know who is attending the session, and even though each attendee may be authorized, a count of access points might give the end user an indication that the session should be terminated or the connection to the network severed. Software programs are also available to monitor at the applications level for members on a network who might be masquerading as an authorized user. For survivability, data at the applications layer should be easily replicated in a secure location and program functionality distributed among several authorized nodes of a network to

minimize the possibility of one failed node stopping the operation in progress. Equally important to survivability is the diversity in processing such that if one program is compromised, the end user could switch to a different mode of an application which may not be compromised, and continue operations while simultaneously discovering the intrusion point and blocking it.

C. SUMMARY

Risk analysis and management of risks identified requires a good understanding of the location of vulnerabilities in the network. To locate possible intruder entrances and paths through the network precisely, a thorough understanding of the layer abstractions assists in defining the vulnerabilities and in mapping out a mitigation strategy that can place the right resources in the right layer abstraction for maximum effectiveness. When considering the vulnerability in a network, it is useful to know which architectural abstraction layer or layers must be penetrated to compromise the networks availability or the data integrity of confidentiality, and to know what the characterization of the penetration might be depending on where the attack is made, and finally what resources are available to protect the Quality of Service in each layer. Knowing where in the layer abstraction the network is most vulnerable, given the value of the data asset remains constant, can support the decision of where to concentrate resources to counter an attack. Equally important in computer network warfare, it determines the ideal location to enter the enemy's network to disrupt their operations if that is a campaign objective and a desired effect.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. OVERVIEW OF SOME CURRENT RISK MANAGEMENT PROCESS MODELS AND THEIR APPLICABILITY TO NETWORKS

A. INTRODUCTION

This appendix explores the methods of risk management processes for network systems used to varying degrees in the commercial and defense market. As DoD continues to formalize their process of managing the risk to the global network system in the GIG and the individual networks now resident in all military organizations, incorporating applicable processes that have made these models successful for other organizations could support DoD's efforts to make their process robust and timely.

A majority of the models explored below are process models and vary between the qualitative and quantitative realms. Qualitative models take a large amount of time and resources, especially human resources to collect and analyze all the data. They can lack specificity and contain much subjective information and opinions. However, when empirical data is unavailable or too difficult to obtain, as in the destructive testing of rare and limited components, a subjective model may be the only path to obtain information about a system and its risk factors. Quantitative models appear on the surface to be more logical and fit into the engineer's idea of accurate information and outcomes. Moreover, they too can produce misleading results if the input data into the model is ambiguous, approximate or inconsistent. Ambiguous data can come from the misidentification of possible outcomes or not fully recognizing all possible outcomes from the implementation of a process model. Approximations are introduced into models by oversimplification of data or model parameters, assumptions introduced, or idealized representations (Ayyab, 2003). In a system as broad in scope and complex as the global connectivity of the GIG (let alone the individual services' networked systems), no one risk assessment process model provides the military a complete representation of the steps to go through to quantify system risk. Nor is it possible for one model provide the information necessary to implement procedures or protection systems and schemes to protect the entire network. That does not mean that the use of risk assessment models in

determining how to protect the GIG and all the systems in a global network can be abandoned. Each model allows some insight into how to structure a risk management system, be it for the enterprise, for a specific theater of operation, a component's partitioned operation in that theater, a weapons platform subsystem, or for a specific application on that platform.

B. DESCRIPTIONS OF CURRENT MODELS AND THEIR APPLICABILITY

1. Information Assurance Risk Management (IARM) (Safety Risk)

The IARM methodology was developed in 2001 by LCDR E. D. Hernandez, a Naval Postgraduate School student, for his thesis work (Hernandez, 2001). The methodology draws on the steps used by the Navy for Operational Risk Management (ORM) as defined in OPNAV 3500.39.B; a framework for evaluating the risks involved in critical operations that pose a safety hazard (e.g., replenishment operations in heavy seas). ORM is a systematic way of discovering and ranking risks of an operation and deciding how to minimize the risk by altering the way the operation is conducted, by taking other safety measures, avoiding risk by not performing the operation, or accepting the risk because the benefits outweigh the risk. IARM is also patterned after Navy-Marine Corps Internet (NMCI) computer network defense model of protect, detect, react, recover and revise and the Defense Acquisition University (DAU) five category risk evaluation matrix card.

The five steps in IARM are the following.

1. Identify vulnerabilities: vulnerabilities are classified according to asset relationship (hardware, software, data, services) and information attributes that could be compromised (confidentiality, availability, integrity).
2. Assess vulnerabilities: a process similar to the DAU risk card is used to rank each vulnerability identified in step 1 as to its likelihood and its severity. Depending on where the vulnerability falls within the matrix, a unit-less number is assigned as a risk level from 1 (most impactful) to 5 (least impactful).

3. Make risk decisions: based on the risk level in the second step, risk assessments are made to determine what would be an acceptable risk based on the benefit, and what risks need to be mitigated or avoided. This is the planning stage for determining the controls necessary to manage the risks identified in step 2.
4. Implement Controls: Installing the controls, either technological or procedural, assigning responsibility, and providing support.
5. Supervise: This stage is the feedback loop of monitoring the results of control implementation. It is also the time to observe if the implementation of controls has had any adverse effect on the assumptions made in previous steps.

The author cites as advantages of IARM over traditional approaches the systematic nature of the method, proactive nature of attempting to discover all threats and vulnerabilities (such as social engineering threats), and increased communication between network users, information systems technicians, and decision makers through a common language of the ranking of risks (Hernandez, 2001). While the claim of a systematic approach is justified, the advantage of capturing all threats and vulnerabilities may be inflated. The process does look at more than just technological controls and digital network threats. However, it is impossible to capture all threats and vulnerabilities in one or even many iterations of a standard process. The system requirements and system capabilities change too quickly as well as the source and nature of threats is continuously evolving with the developing technologies.

2. Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM)

CRAMM is a process model owned by the Government of the United Kingdom that follows a three step process. It relies heavily on qualitative data gathering and analysis from subject matter experts and interviews with computer system operators. The steps in the process are the following.

1. Building an asset model and defining system boundaries
2. Asset dependencies are established and a threat and vulnerability assessment is made by circulating questionnaires. With the software tool, measures of risk are calculated.

3. With a comprehensive countermeasure database, the tool recommends the countermeasures (policies and technical tools) that should be implemented to mitigate the risk.

Data gathered is placed into a software program that can produce reports to management on asset classes, threats and vulnerabilities, and countermeasures to deploy. The model has been around since 1985 and is difficult to use unless the organization has someone who has used the model in the past. CRAMM does allow the organization to systematically think about what the value of their information is and what steps need to be taken to address vulnerabilities against known threats. Not much information exists on what to do about unknown threats and how to address them as they are identified through threat libraries or if one penetrates the organization's system (Jones & Ashenden, 2005).

3. Fundamental Information Risk Management (FIRM)

FIRM is a two-phase, ten-stage process that looks at the information systems and networks of an organization from a very high level. It is a quantitative data gathering and scoring process with some software tools for organizing data gained through "scorecards," which are filled out by resource owners. The idea is to take the scorecards and balance out the system functionality with system protections and produce a senior management report as to the state of vulnerability and protection of the organization's system enterprise. The two phases are designed to get senior-level buy-in by showing ways to plug obvious but overlooked vulnerability holes. The second phase collects information about the enterprise a second time with a more detailed look at the score, or assets versus threats and vulnerabilities. By virtue of distributing quantitative data gathering among all the organization's resource managers, this process appears to work better in larger organizations. It does not take the next step of identifying and recommending countermeasure implementation (Jones & Ashenden, 2005).

4. Simple to Apply Risk Analysis (SARA) and Simplified Process for Risk Identification (SPRINT)

The SARA and SPRINT tools are complementary and the process is similar to the processes above in that they rely on collecting data through interviews with management, system operators and subject matter experts. SPRINT is a fast track tool that assesses the

business risk, the threats, and system vulnerabilities and controls through mediated interviews. The goal after assessment is to produce a plan to implement system controls that more effectively reduce the assessed risk. SARA is designed for business-critical systems and uses a more in depth approach than SPRINT. SARA uses interviews and workshops to 1) define the system and its boundaries, 2) identifying business requirements for security, 3) assessing threats and vulnerabilities in a workshop format, and 4) production of an action plan. These tools are labor intensive and require the time and manpower of a significant part of the organization (Jones & Ashenden, 2005).

5. Cobra

Cobra is a process similar to CRAMM and is owned by a security service in the United Kingdom as well. While the process is similar to CRAMM, it makes extensive use of questionnaires to gather data and the software tool is modularized to conduct assessments on certain aspects of security in isolation. For a full assessment, the modules are combined for a full report on the risk condition of the enterprise and countermeasure to implement (Jones & Ashenden, 2005).

6. The CORAS Method

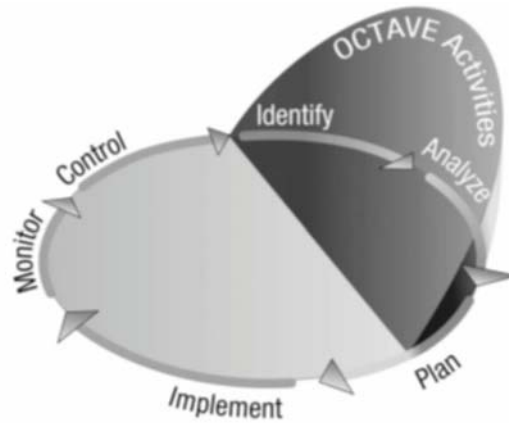
Another United Kingdom funded project, CORAS (an undefined acronym) is a risk management method that uses a Unified Modeling Language (UML) in its automated tool, which supports a methodology similar to the process models above. The method follows the process of 1) identifying security-critical assets through a questionnaire and accurately representing the current system's security state and the interaction between system components, 2) risk identification by determining threats (through fault trees and Failure Mode, Effects and Criticality Analysis {FMECA}), 3) risk analysis through identification of outcomes and consequences and the likelihood of the outcomes, 4) risk evaluation by ranking the risks according to likelihood and evaluating the impact of the consequences determined in step 3, and 5) risk treatment in the form of mitigation or avoidance/transference strategies by employing countermeasures to reduce the likelihood or reduce the consequences. Throughout the process steps, the model specifies strong

communication between teams conducting the analysis and constant monitoring and review of results so that the model can be adjusted in an iterative fashion (Hamdi & Boudriga, 2005).

The next three process models were developed by the CERT® Coordination Center, which is part of the Software Engineering Institute, Carnegie Mellon University; a federally funded research and development center sponsored by U.S. DoD. The primary objective of CERT is to develop technology and systems management practices to resist attack to computer network systems and to limit damage and ensure continuity of critical services when an attack on a network occurs.

7. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)

This process model and its associated software were developed by the Carnegie Mellon University and Software Engineering Institute and use the workshop format to define the assessment and gather data. The process is designed to bring all facets of a business together through interdisciplinary teams that look at risks from threats and vulnerabilities to the organization not only in information systems, but in all facets of a business. The process model is run in three phases; 1) asset prioritization through data gathering, 2) assessment of threats and vulnerabilities and where these impact information flow and veracity through workshops, and 3) Risk identification and development of mitigation strategies. One of the terminal objectives of the OCTAVE process is to develop threat profiles for individual assets. This takes into account both threat access ability (through vulnerabilities and other means) and a threat motivation profile. This method is unique to OCTAVE over the other previous models, but is a theme used in some of the later models examined.



The CERT Coordination Center's OCTAVE model follows many of the characteristics of the DoD Risk Management Process for Acquisition Programs

Figure 19. The OCTAVE Risk Management Cycle (From: Caralli & Young, 2008)

New versions of the OCTAVE method and tool have been developed since OCTAVE was created in 1999 including a small business version and a “continuous improvement” version. The same methodology of inter-active team workshops is employed by the newest version, but concentrates on information asset storage, transmission, and use to allow assessments to be conducted without professional knowledge of assessment processes. The aim is to broaden the landscape assessed by opening up the assessment process to operational security, not just information security. The shift from periodic risk assessment to a continuous action was prompted by the dramatic changes in information ownership and use through networked systems just in the last decade. New terms have been developed including Continuous Risk Management (CRM) and Operational Risk Management (ORM), although this is not a new term to Naval safety programs (Caralli & Young, 2008). The OCTAVE developers have expressed the need for a continuous program in the following statement.

Operational resiliency in an organization is dependent on many types of organizational assets performing together to achieve a mission. (Caralli & Young, 2008, p. 78)

8. Architecture Refinement Process

This model, created by Robert Ellison and Andrew Moore (Ellison & Moore, 2001) from the Software Engineering Institute of Carnegie-Mellon University (SEI/CMU) CERT Coordination Center, is tailored more toward the concept definition, design, and development stage of a system lifecycle and concentrates on architecting a system for survivability. Consistent with other models in the architecting of software-based systems, they employ the spiral model from a systems engineering standpoint. In fact, the process is the successive use of four models/processes, which comprise the four quadrants of a spiral graph. Counter to some developers concentrating their architecture on the arrangement of technological security components, this model seeks to address how the system architecture counters attacks that degrade the system's mission; in other words, how to architect for survivability. The authors define survivability similar to the definitions of Chapter V in that survivability is the characteristic of a system to perform its designated mission even when penetrated and compromised by a hostile force. The survivability of a system is impacted by the system's reliability, performance, safety, security and fault tolerance.

Similar to the military's Observer, Orient, Decide, Act (OODA Loop) the Plan Decide, Execute (PDE Cycle), the spiral process of this model leads the developer through architecting the defense of a system in a Resist, Recognize, Recover continuum, which employs reusable survivability design primitives. Examples of these design primitives are replication, redundancy, distribution, separation access control, intrusion detection, diversity, and adaptive reconfiguration. The reuse of these primitives comes in an iterative fashion as the architect works through each cycle of the spiral. The four quadrants of the spiral are the following.

1. Survivability Planning; including mechanism-based risk remediation
2. Usage Modeling; essential work-flow analysis
3. Intrusion Modeling; using attack trees and intrusion work-flow models. (An intrusion work-flow model is simply a path through an attack tree diagram to show what path an intruder might take to exploit vulnerabilities in the networked system.)
4. Survivability Risk Analysis; vulnerability and impact assessment

The process starts with designing the system architecture around survivability design primitives based on the current knowledge of the system requirements and the adversarial environment. The usage modeling refines the architecture around essential work flows. A model of intrusion to the architected network is built with an attack tree analysis of possible intrusions and their cascading effect on the architected network, and finally, a survivability risk analysis is conducted based on the intrusion model to determine where the architecture needs to be refined for survivability; allowing essential services to recover or continue operating to meet the system's mission. The process of this model is shown in three iterations: firstly, considering network-based attacks, secondly, application-based attacks are contemplated, and finally, data-centered attacks are analyzed. Each iteration considers the correct architecting of the system for survivability using the survivability design primitives that preserves the quality attributes of the system of performance and reliability (Ellison & Moore, 2001).

The penultimate survivability primitive above is a topic of some controversy. In their article about the unwarranted concern of not diversifying, Fred Schneider and Ken Birman from Cornell University postulate that diversity, especially in software, can be too expensive and makes a system too complex for the advantage gained by a network attacker who gains only slightly by the similarity in software systems in a monoculture environment (Schneider & Birman, 2009).

9. Mission Assurance Analysis Protocol (MAAP)

Another process model developed by SEI/CMU is the Mission Assurance Analysis Protocol or MAAP, a process contained in the SEI Mission-Oriented Success Analysis and Improvement Criteria (MOSAIC) management approach. MAAP is more of a general method of looking at distributed, complex systems within an organization to discover the elements which make it successful and mitigating the factors that deter success. The process is comprised of building a model (representation) of the current state of a system in terms of its ability to achieve mission success. The uncertainty (probability) of achieving objectives due to inside or outside influences is analyzed along with the categorization of the threats (reliability issues, unintended mistakes, intrusions)

that would hinder success. The MAAP protocol is a roadmap for conducting the analysis by assigning activities, goals, and expected outcomes. Risk plays into this model in the consideration of the uncertainty of factors that would inhibit success. As with process models explained above, this process is time and manpower intensive, with the formation and training of teams from within and organizations to conduct the process. The requirements for being on a team are an in-depth knowledge of the system being considered and an understanding of risk assessment, process modeling, and statistics. The qualifications seem to indicate that a team with all members of this caliber would be difficult to assemble for just one part of a distributed system, let alone the entire network.

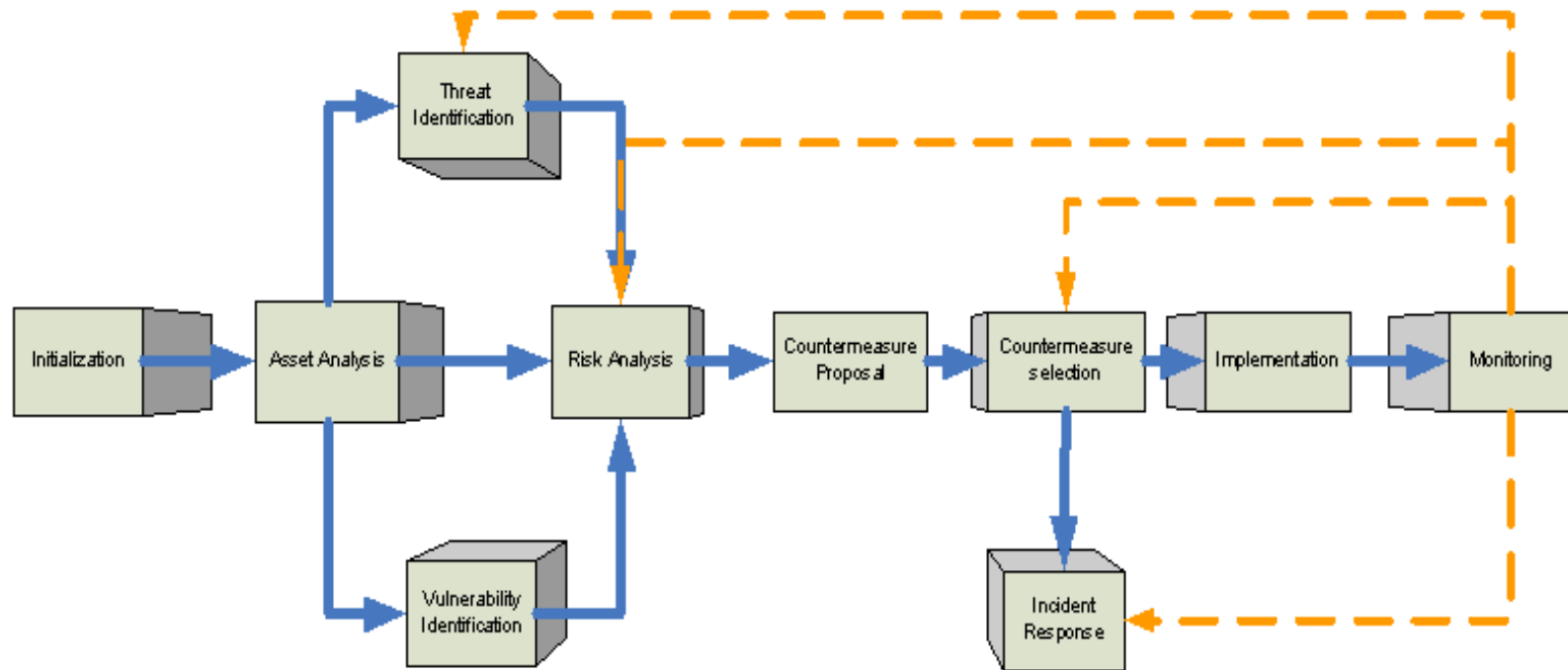
The end product of a MAAP assessment yields a success profile for every key objective determined during the operational model development. Each key objective success profile informs the organization of their probability of mission success in that key objective, and for key objectives not acceptable to the organization; a plan can be developed to remediate the influences causing a less than desired success rate. Interestingly, the operational model development is different than the asset valuation of models above because it focuses not so much on value but more on the contribution each element in the distributed system makes to overall mission success. The decomposition of each key objective into influences and their uncertainties requires a disciplined approach to determining threats and vulnerabilities (Alberts et al., 2008).

MAAP is primarily a management process, designed to take a holistic view of a complex and distributed system. While the description of the MAAP process does not explicitly state that it is a risk management model for computer networks, the fact that it was developed by SEI/CMU seems to indicate that the motivation was to use this process in a software-driven computer network environment. In fact, SEI/CMU has piloted the protocol in a cyber-security incident response system and in elements of software development and deployment.

10. Network Risk Analysis Method (NetRAM)

This framework for risk management was developed by M. Hamdi and N. Boudriga of the University of Tunis (Hamdi & Bordiga, 2005). Their motivation in

developing this method was to develop a structured framework that captures risk management approaches, techniques, and software tools that can be used by an organization to run an effective risk management program. Their methodology centers on risk management analysis, decision, and response. The model consists of a ten-step recursive process that includes pathways to return and adjust previous steps based on information revealed during a later step. Included in one of their model steps are a robust process for incident impact and response, particularly framing the response to maximize recovery and minimize reduction in critical services and safety issues. The model is scalable to different types and sizes of network architectures and topologies, and is designed to remain current with changing technologies with a learning process that updates quantitative parameters and semantic links. A set of modules in the software tool also monitors the system's states to detect deviations from normal and differences in values of key parameters. One of the unique features claimed by the authors is that their methodology restricts the propagation of errors or poor decisions made in previous steps of the methodology.



The NetRAM model includes a process for evaluating risk based on the networks ability to react to attacks that are experienced; a measure of resiliency.

Figure 20. The 10 Modules of the NetRAM Framework (From: Hamdi & Bordiga, 2005)

Aside from the fact that this model looks quite similar to the ones above and uses some of the same methodologies for determining threats and assessing vulnerabilities (a combination of questionnaires and automated vulnerability scanners), the separation between preventative and reactive risk analysis is one area that stands out. While preventative analysis studies the likelihood of threats exploiting vulnerabilities with a resultant undesired effect, reactive analysis considers the probability of the detection system alerting on a network intrusion, following the amount of penetration, and the effects on system operation, particularly critical operations. This is the idea behind a consequences-based risk management approach. While full efforts should still be directed at prevention, it is inadvisable to give short shrift to planning the reaction and recovery from an unknown threat, left to exploit the vulnerability that remained undetected and unprotected. In addition, an important element in reactive risk management is the real-time element of recovery and an analysis on the system of the time requirements for recovery to limit system functionality or to meet critical mission objectives.

11. Mission Oriented Risk and Design Analysis (MORDA)

The MORDA methodology was developed to address the risk involved in the operation of DoD's Global Command and Control System (GCCS) from the war fighter's perspective. The methodology employs a model called Security Optimization Countermeasure Risk and Threat Evaluation System (SOCRATES). The MORDA methodology and the SOCRATES model ride on the foundation of the following.

- Attack tree models
- Qualitative information assurance models
- Quantitative information assurance models
- Multiple objective decision analysis models for information assurance; using values rather than alternatives to measure parameters

It is built within the DoD's Information Assurance Technical Framework (IATF), which is what the DoD has developed as the architecture for information assurance systems implemented on a DoD network. The decision to use the word design in the

model's name was prompted by the developers' opinion that a system of risk assessment and management of risk needed to start in the design phase of a system, not when the system reached the operational phase of the system lifecycle.

SOCRATES is a quantitative design optimization model that uses multiple objective decision analysis as a mathematical technique for optimizing the countermeasure design of a system. Input into the model is data about the adversary provided by threat experts, the attack profile provided by security experts using attack tree analysis, and the countermeasure characteristics and design options provided by systems engineers. Input data is entered into three value models; adversary model, user model, and service provider model. Using multiple objective decision analysis, value goals are matched to value measures (constructive units are developed if no natural units exist), and the value measures are weighted. The competing objectives, now value measured and weighted, are compared by a weighted sum such that:

$$v(x) = \sum_{i=1}^n w_i v_i(x_i) \quad (1)$$

where:

$v(x)$	value of alternative
$i = 1 \text{ to } n$	numbered value measures
x_i	score of the alternative on the i^{th} value measure
$v_i(x_i)$	a single-dimensional value of a score of x_i
w_i	weight of the i^{th} value measure (all weights sum to 1) (Buckshaw et al., 2005, p. 23).

This yields the optimum alternate within a set of competing objectives. To explain the value system, an adversary value model would use attack data based on the adversary's motivation for the attack, the adversary's assumption as to how likely the attack would succeed, how likely the adversary or the attack would be detected, the adversary's resource consumption in executing the attack, and the impact on the system

should the attack succeed. Different techniques are employed to produce the initial value goals and measures including affinity diagrams. Some assumptions of the models are that it is better to measure attack preferences instead of probabilities, that the adversary is a rational thinker, and that an adversary is going to try to maximize their benefit and maximize the impact of their attack while minimizing resource expenditure.

The user value model is structured similarly, and the value measure is defined by the values of achieving an objective of the war fighter. The competing objectives are the limitations on the system using alternative countermeasures and the effect on mission accomplishment.

The value models' results are input into an Integration and Analysis model, which determines the value of an operable system to the war fighter considering the cost/benefit and constraints on the use of the best value countermeasure alternatives determined in the value models. The integration takes the countermeasure alternative that best counters the adversary and compares it to the degradation in value (mission accomplishment) to the user community. This, along with the service provider value model (which is important to the service providers), yields $\Delta v(x)$; a comparison of alternatives that match adversary, user and service provider values to determine the best alternative. When processed through a cost benefit model, and evaluated as to the resources required to implement, an architectural framework of countermeasures can be developed in the design of a new system or as a modification to an existing system (for instance GCCS). The final step in the methodology is to optimize the system value as constrained by system cost and countermeasure compatibility.

The authors believe there are advantages to their model and methodology over other models in that it explicitly describes the sequence of attacks and compares the motivation behind certain attack strategies. It also takes into consideration the conflicting objectives and the interdependencies of all the variables, and sets a framework for allocating resources best aligned for mission accomplishment.

C. SUMMARY

A common thread in all the process models discussed above is the necessary involvement of the entire organization in the process, from top level management to the network administrators and functional managers. Executives need to take an on-going role in the security and risk management process of one of their most valuable assets. “It is now recognized that network security is a mainstream business process, which can only be mandated and directed by senior management” (Adler & Lepofsky, 2000, p. 38).

All of the models either allude to or directly state that risk management is an iterative and continuous process. A static plan, just like the technology of today, is outdated in short order. Unless the value of the information in the system, the changes in system vulnerabilities, and the threat to information system assets and the operations they support is not continually reviewed for necessary changes to network technology and personnel policies and procedures, the value of the network rapidly declines as the system becomes increasingly susceptible to attack from competitors and adversaries.

APPENDIX C. FORMULATION OF THE COST/BENEFIT MODEL FOR REACTIVE RISK ANALYSIS

A. MODEL DERIVATION

Hamdi and Bordiga developed a cost/benefit model that can be used to analyze a set of Intrusion Detection Systems (IDS) and reactive countermeasures to support decisions on the type and quality of IDS and countermeasure required to counter a given set of attacks on a network. In this model (Hamdi & Bordiga, 2005), the probability of attack is not considered, since it is an analysis of effects on the network when attacks of a given set are conducted against the network. The analysis provides a cost/benefit analysis of the set of IDS and countermeasures given the set of attacks and the effects/consequences of the impact on the network from the attacks. The analysis gives a relative measurement of the cost and benefit to network survivability and resiliency for a set of IDS and countermeasures installed on the network. The network architects can compare different sets of IDS and countermeasures that fit within the budget to maximize the survivability benefit to the network. The model uses four factors to analyze for the cost and benefit of a given set of IDS and countermeasures. They are as follows.

Detection cost is the set of costs for every IDS/analyzer installed on the network, whether a particular IDS is used against an attack or not (an IDS is composed of a network traffic sensor and an analyzer to interpret data from the sensor. In this analysis, the authors use the term “analyzer” to denote the entire IDS). The cost is a given and is scaled appropriately for the units of the whole model. Detection cost is depicted as γ_{Ai} , i contained in $\{1, \dots, n_A\}$ for n_A analyzers.

Reaction cost is also given and scaled the units of the analysis for each countermeasure that provides a reaction to an attack and is depicted as γ_{rk} , for each reaction r_k for all k contained in $\{1, \dots, n_r\}$ for n_r countermeasures.

Impact of a given attack i_{aj} causes various effects on the network from attack a_j . The effects of the attack, which represent multiple attributes, are represented by the term

i_{aj} and a unique term λ_{aj} is developed called the progression factor. A progression factor is included to incorporate the cost or benefits realized by the type of progression that attack is characterized by, for instance, if the attack is stopped before complete execution and the entirety of the attack impact effects are felt on the system, or if the attack is allowed to complete execution, the ability of the countermeasures to recover the network in time to continue required operation. The progression factor is determined by the effectiveness of the countermeasures to stop the attack and recover the network. Impact is modeled as a function of the progression factor where $i_{aj}(1) - i_{aj}(\lambda_{aj})$ is the benefit to the network from the progression factor and $i_{aj}(1)$ is the maximum damage from attack a_j . Thus, $i_{aj}(\lambda_{aj})$ is the cumulative sum of elementary impacts of attack a_j in the interval $[0, \lambda_{aj}]$ such that:

$$i_{aj}(\lambda_{aj}) = \int I(\lambda t_0) d\lambda \text{ over } [0, \lambda_{aj}] \quad (1)$$

“ I ” is defined as the impact function over time as the attack progresses. $I(t)$ can be any function given the type of attack; constant $I(t) = I_0$ if $0 \leq t \leq t_0$, or linear, or any function that defines the progression of the impact over time. In addition, t_0 is the maximum tolerated time the network is allowed to be down and still be considered survivable.

Intrusion Detection System (IDS) efficiency is formulated as follows. The authors define ‘D’ contained in the binary set $\{0, 1\}$, as the probability of detecting an attack; 0 if no attack is detected and 1 if an attack is detected. They define ‘A’ contained in the binary set $\{0, 1\}$ as the probability of an attack; 0 if no attack takes place and 1 if the network is attacked. Efficiency of the IDS can be measured by the conditional probabilities.

- $P(D|A)$ represents a true positive, estimated by sending contaminated packets past IDS
- $P(D|A)$ represents a false positive
- $P(\bar{D}|A)$ represents a false negative
- $P(\bar{D}|\bar{A})$ represents a true negative; no detection, no attack (Hamdi & Bordiga, 2005)

B. MODEL FORMULATION

When considering costs, the authors do not specify the units, but mention that the costs could be monetary or a measurement of resource consumption. The cost to the system of a reaction to a given attack is the probability of detecting a true attack times the cost of the IDS analyzer, the cost of the reaction and the cost of the impact as modified by the benefits of the reaction. It also includes the cost of the IDS analyzer, the cost of the reaction times and the probability that the system makes a false positive detection. Considering an analyzer, A_i , that alerted on attack a_j , the **cost** of performing response r_k to stop the attack is $\gamma(r_k, \lambda_{aj})$ such that:

$$\gamma(r_k, \lambda_{aj}) = (\gamma_{Ai} + \gamma_{rk} + i_{aj}(\lambda_{aj}))P(D|A) + (\gamma_{Ai} + \gamma_{rk})P(\bar{D}|A). \quad (2)$$

The **benefit**, $\beta(r_k, \lambda_{aj})$, to the system of a given reaction to a given attack, is the probability that the analyzer detects the attack times the benefit defined above (impact without progression factor minus impact with progression factor) such that:

$$\beta(r_k, \lambda_{aj}) = (i_{aj}(1) - i_{aj}(\lambda_{aj}))P(D|A). \quad (3)$$

In other words, the reaction to the attack modifies the total attack impact from the start of the impact until the reaction has stopped the attack (Hamdi & Bordiga, 2005). This model takes into account some important elements of gauging the survivability of a networked system; however, it can be challenging to produce empirical quantities for the costs of IDS systems, the costs of reaction countermeasures, and a quantitative value for each element of an attack, i_{aj} and the progression factor, λ_{aj} , which mitigates the effect

of the attack. The value that is most likely the easiest to obtain is a value for IDS efficiency as defined above. This value can probably be obtained through extensive testing against known attacks. However, even this value may not be independent of other components and their use in a network system.

Even more challenging for the network developer, or the engineer who is designing network connectivity between existing information systems, is the balancing act between network costs and network capability to meet requirements. As mentioned in the main body of the thesis, it is difficult to define a set of survivability requirements as they are driven by the scenario (or attack-specific).

Perhaps the value in a network cost/benefit model such as this one is that it supports the development of survivability requirements. They can then be added to the capability requirement's definition as determined by the systems engineering process used, and they can shape the architecture that defines the network composition, both from a hardware standpoint and from the software components developed or applied for reuse.

LIST OF REFERENCES

- Adler, T., & Lepofsky, R. (2000, November). E-accountability: Why network security is an executive function. *CMA Management*, 74(9), 38-40. Retrieved May 1, 2009, from ABI/INFORM Global database. (Document ID: 64743559).
- Alberts, C., Dorofee, A., & Marino, L. (2008). *Preview of the Mission Assurance Analysis Protocol (MAAP): Assessing risk and opportunity in complex environments*. Carnegie Mellon Software Engineering Institute; Technical Note CMU/SEI-2008-TN-011.
- Anderson, F., Budgor, A., Davis, M., & Green, R. (2008). *Enterprise software/SOA IA/security approach (AKA - clarifying the "Fog of SOA IA")*. A Collaborative Position Paper between SPAWAR 5.1.8 and Worldwide Consortium for the Grid. Unpublished.
- Anderson, R. H., & Hundley, R. O. (1998). *The implications of COTS vulnerabilities for the DoD and critical U.S. infrastructures: What can and should the DoD do?* Santa Monica, CA: Rand Corporation.
- Ayyub, B. M. (2003). *Risk analysis in engineering and economics*. Boca Raton: Chapman & Hall/CRC.
- Birman, Kenneth P. (2009). *A History of the virtual synchrony replication model*. Retrieved July 7, 2009, from <http://www.cs.cornell.edu/ken/History.pdf>
- Blanchard, B. S., & Fabrycky, W. J. (2006). *Systems engineering and analysis* (4th ed.). Upper Saddle River, New Jersey: Pearson, Prentiss Hall.
- Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M., & Saydjari, O. S. (2005). Mission oriented risk and design analysis of critical information systems. *Military Operations Research*, 10(2), 19-38.
- Caralli, R., & Young, L. (2008). *Expanding the OCTAVE method to perform continuous risk management of information and operational security*. 2008 CERT Research Annual Report; Software Engineering Institute, Carnegie Mellon. Retrieved July 5, 2009, from <http://www.cert.org/research/2008research-report.pdf>
- CERT. (2008). Insider threat research: Our work. *Insider Threat* [Web site]. Retrieved July, 18, 2009, from http://www.cert.org/insider_threat/more.html
- Chen, D., Garg, S., & Trivedi, K. S. (2002, September 28). *Network survivability performance evaluation: A quantitative approach with applications in wireless ad-hoc networks*. *MSWiM'02*, 61-68.

- Chittister, Clyde G., & Y. Y. Haimes. (2006). Cybersecurity: From ad hoc patching to lifecycle of software engineering. *Journal of Homeland Security and Emergency Management*, 3(4), Article 3, 1-20. Retrieved August 1, 2009, from <http://www.bepress.com/jhsem/vol3/iss4/3>
- Clark, D. D., Sollins, K., Wroclawski, J., and Faber, T. (2003). *Addressing reality: An architectural response to real-world demands on the evolving Internet*. In Proceedings of SIGCOMM 2003, workshop on Future Directions in Network Architecture, pp. 247-257, August 2003. Retrieved August 2, 2009, from <http://groups.csail.mit.edu/ana/Publications/index.html>
- Clemen, R. T., & Reilly, T. (2001). *Making hard decisions with decision tools*[®]. Australia: Duxbury Thomson Learning.
- Davis, M. (2008). *Enterprise IA/security/cyber risk assessment: An overall "protections" approach*. (Draft). Space and Naval Warfare Command (SPAWAR 5.8/5.0.6).
- Defense Information Systems Agency. (2009). *Press release: Host based security systems*, Retrieved May 23, 2009, from <http://www.disa.mil/news/pressresources/factsheets/hbss.html>
- deJong, Edwin. (2009, August). Middleware offers integration framework for dynamic UAV applications. *Defense Tech Briefs*, 3-6.
- Department of Defense. Office of the Undersecretary of Defense (AT&L). Systems and Software Engineering/Enterprise Development. (2006). *Risk management guide for DoD acquisition, sixth edition (version 1.0)*.
- Department of Defense/Chief Information Officer. (2007). *Department of defense global information grid architectural vision: Vision for a net-centric, service oriented DoD enterprise version 1.0*. Retrieved April 25, 2009, from www.defenselink.mil/cio-nii/GIG/ArchVision.pdf
- Department of the Navy. (2008). *Naval SYSCOM risk management policy*; NAVSEAINST 5000.8. (Naval Directive).
- Ellison, R. J., & Moore, A. P. (2001). *Architectural refinement for the design of survivable systems*. Carnegie Mellon Software Engineering Institute; Technical Note CMU/SEI-2001-TN-08.
- Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., Longstaff, T., & Mead, N. R.. (1999). *Survivable network systems: An emerging discipline*. Carnegie Mellon Software Engineering Institute; Technical Note CMU/SEI-97-TR-013.

- Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., Mead, N. R., & Moore, A. P. (2009). *Foundations for survivable systems engineering*. [CERT Web site]. Retrieved September 2, 2009, from http://www.cert.org/archive/html/SSE_foundations.html
- Faber, S. (2007). *Leaking private IP information: AS112 DNS traffic analysis*. 2007 CERT Research Annual Report. Software Engineering Institute, Carnegie Mellon. Retrieved July 5, 2009, from <http://www.cert.org/research/2007research-report.pdf>
- Gehlot, Vijay. (2009). *CSC 9010 service oriented architecture design and Analysis: introduction*. [Slides]. United States: CSC Villanova University. Retrieved September 3, 2009, from <http://www.csc.villanova.edu/~gehlot/9010/lec/Intro.pdf>
- Germain, J. M. (2008). The winds of cyber war. *TechNewsWorld*. Retrieved April 29, 2009, from Linux Insider <http://www.linuxinsider.com/story/64494.html?wlc=1240179703>
- Haimes, Y. Y. (2007). *Systems-based risk assessment and management*. [Slides]. United States: Naval Postgraduate School.
- Haimes, Yacov Y. (2009). *Risk modeling, assessment, and management*. New Jersey: John Wiley and Sons, Inc.
- Hamdi, M., & Boudriga, N. (2005). Computer and network security risk management: Theory, challenges, and countermeasures. *International Journal of Communication Systems*, 18, 763–793.
- Heegaard, P. E., & Trivedi, K. S. (2009). Network survivability modeling. *Computer Networks*, 53, 1215-1234. (Document Number 53768584)
- Hernandez, E. D. (2001). *Using Operational Risk Management (ORM) to improve Computer Network Defense (CND) performance in the Department of the Navy*. Master's Thesis, Naval Postgraduate School, Monterey, CA.
- Hight, B. (2004). *Navy vision for FORCENet to support joint functional capabilities*. [Slides]. United States: Chief of Naval Operations (N61R) Briefing to NDIA Science & Engineering Technology Conference, April 22, 2004. Retrieved July 7, 2009, from <http://www.dtic.mil/ndia/2004tech/hight.ppt>
- Hunerwadel, J. P., Lt Col, USAF (Ret). (2006, Spring). The effects-based approach to operations; questions and answers. *Air & Space Power Journal*. Retrieved September 5, 2009, from <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj06/spr06/hunerwadel.html>
- Ingoldsby, Terrance R. (2009). *Attack tree-based risk analysis: The integrated modeling of hostile and random threats*. [Slides]. Canada: Amenaza Technologies Limited.

- Jones, A., & Ashenden, D. (2005). *Risk management for computer security: Protecting your network and information assets*. Amsterdam: Elsevier Butterworth-Heinmann.
- Joseph, D., & Stoica, I. (2008, September/October). Modeling middleboxes. *IEEE Network*, 20-25. Retrieved May 1, 2009, from <http://ieeexplore.ieee.org/Xplore/guesthome.jsp>
- Kioskea.net. (2009). *What does topology mean?* Retrieved August 2, 2009, from <http://en.kioskea.net/contents/initiation/topologi.php3>
- Kujawski, Edouard. (2009). *Risk analysis and management for engineering systems. Module 9: Enterprise risk management*. [Slides]. United States: Naval Postgraduate School.
- Mahmoud, Qusay. (2005). Service-Oriented Architecture (SOA) and web services: The road to enterprise application integration. *Sun Developer Network* [Web site]. Retrieved August 2009, from <http://java.sun.com/developer/technicalArticles/WebServices/soa/>
- Maier, Mark W., & Rectin, Eberhardt. (2002). *The art of systems architecting*. Boca Raton: CRC Press.
- May, M. (2004). A layered network architecture and implementation for Ethernet services. *Fujitsu Network Communications, Inc.* Retrieved August 6, 2009, from http://www.fujitsu.com/downloads/NC/Whitepapers/layered_network_wp.pdf
- McCabe Software. (2009). *Uncover software security vulnerabilities off the beaten path*. [Web page]. Retrieved August 14, 2009, from http://www.mccabe.com/contact_securityWebSeminar.htm
- Mulokey, William P. (2009). Using the U.S. Department of Defense architecture framework to build security into the lifecycle. *Insight*, 12(2), 27-29.
- National Security Agency. Central Security Service. (2005). *Router security configuration guide supplement*. Retrieved April 25, 2009, from <http://www.nsa.gov/ia/files/routers/c4-040r-02.pdf>
- National Security Agency. Central Security Service. (2008). *Global information grid: The GIG vision-enabled by information assurance*. Retrieved April 25, 2009, from http://www.nsa.gov/ia/programs/global_industry_grid/index.shtml
- National Security Agency. Central Security Service. (2008). *Router security configuration guide supplement-security for IPv6 routers*. Retrieved April 25, 2009, from <http://www.nsa.gov/ia/files/routers/I33-002R-06.pdf>

- National Security Agency. Central Security Service. (2009). *Network anomaly detection algorithm*. Retrieved April 25, 2009, from http://www.nsa.gov/research/tech_transfer/fact_sheets/network_anomaly_detection.shtml
- National Security Agency. Information Assurance Directorate. (2008). *Net-Centric Enterprise Services (NCES) profile of eXtensible Access Control Markup Language (XACML) for Role Based Access Control (RBAC)*. Retrieved April 25, 2009, from http://www.nsa.gov/ia/_files/SAML_Profile_20080716.pdf
- National Security Agency. Information Assurance Directorate. (2008). *Net-Centric Enterprise Services (NCES) profile of web services security: Simple Object Access Protocol (SOAP) Message Security (WSSE)*. Retrieved April 25, 2009, from http://www.nsa.gov/ia/_files/SAML_Profile_20080716.pdf
- National Security Agency. Information Assurance Directorate. (2005). *Network hardware analysis and evaluation division systems and network attack center recommended 802.11 wireless local area network architecture*. (Document ID: I332-008R-2005). Retrieved April 25, 2009, from http://www.nsa.gov/ia/_files/wireless/I332-008R-2005.pdf
- National Security Agency. Systems and Network Attack Center (SNAC). (2001). *The 60 minute network security guide; (First steps towards a secure network environment)*. Retrieved April 25, 2009, from http://www.nsa.gov/ia/_files/support/I33-011R-2006.pdf
- National Security Agency/Systems and Network Analysis Center/Information Assurance Directorate. (2006). *Desktop or enterprise firewall?* Retrieved April 25, 2009, from http://www.nsa.gov/ia/_files/factsheets/I73-002-06.pdf
- Naval Surface Warfare Center Dahlgren Division. (2004). *Open Architecture (OA) computing environment technologies and standards; Version 1.0*. Retrieved June 28, 2008, from http://www.nswc.navy.mil/TIE/OACE/docs/OACE_Tech_Std_v1dot0_final.pdf
- Scherrer, A., Borgnat, P., Fleury, E., Guillaume, J-L, & Robardet, C. (2008). Description and simulation of dynamic mobility networks. *Computer Networks*, 52(15), 2842. Retrieved May 1, 2009, from ABI/INFORM Global database. (Document ID: 1562045021).
- Schneider, B. (2001, May). Network security: It's not about the technology. *CIO*, 14(14), 166. Retrieved May 1, 2009, from ABI/INFORM Global database. (Document ID: 73022124).
- Schneider, F. B., & Birman, K. P. (2009, January/February). The monoculture risk put into context. *IEEE Security and Privacy*, 14-17. Retrieved July 7, 2009, from <http://www.cs.cornell.edu/projects/Quicksilver/>

- Smith, Ryan. (2003). *OSI Model-Part Two*. *ServerWatch*. [Web site]. Retrieved August 2009, from <http://www.serverwatch.com/tutorials/article.php/1474881/The-OSI-Model---Part-Two.htm>
- Sterbenz, J. P. G. (2006). *High speed networking tutorial: Network architecture and topology*. [Slides] Retrieved August 2, 2009, from <http://www.sterbenz.org/jpgs/tutorials/hsn/tut3-hsn-display.pdf>
- Stewart, F. M. (2006). *2006 CCRTS: The state of the art and the state of the practice FORCEnet net centric architecture—A standards view*. Space and Naval Warfare Systems Command Decision Paper. Retrieved July 7, 2009, from http://www.dodccrp.org/events/2006_CCRTS/html/papers/024.pdf
- Storey, Neil. (1996). *Safety-critical computer systems*. Harlow, England: Pearson-Prentice Hall.
- United States Government Accountability Office. (2004). *Report to subcommittee on terrorism, unconventional threats, and capabilities, committee on armed services, house of representatives: Defense acquisitions; The global information grid and challenges facing its implementation*. (Document Number: GAO-04-858). Retrieved May 23, 2009, from <http://www.gao.gov/new.items/d04858.pdf>
- Walker, Julianne. (2008). Hash tables. *Eternally Confuzzled*. [Web site]. Retrieved August 2009, from http://www.eternallyconfuzzled.com/tuts/datastructures/jsw_tut_hashtable.aspx

INITIAL DISTRIBUTION LIST

- 1 Defense Technical Information Center
 Ft. Belvoir, VA
2. Dudley Knox Library
 Naval Postgraduate School
 Monterey, CA
3. Dr. Edouard Kujawski
 Naval Postgraduate School
 Monterey, CA
4. Ms. Jean Johnson
 Naval Postgraduate School
 Monterey, CA
5. Mr. Bob Stephenson
 Commander, U.S. Pacific Fleet (N6T)
 Pearl Harbor, HI
6. Mr. Jim Williams
 Commander, U.S. Pacific Fleet (N6T1)
 Pearl Harbor, HI